OUR CUSTOMER TERMS
CLOUD SERVICES - TAILORED INFRASTRUCTURE

CONTENTS

OUR CUSTOMER TERMS
CLOUD SERVICES - TAILORED INFRASTRUCTURE

OUR CUSTOMER TERMS
CLOUD SERVICES - TAILORED INFRASTRUCTURE

Certain words are used with the specific meanings set out in the General Terms part of Our Customer Terms at http://www.telstra.com.au/customer-terms/business-government/cloud-services/, or in the General Terms of Our Customer Terms at http://www.telstra.com.au/customer-terms/business-government/index.htm

1 APPLICABLE TERMS

1.1 In addition to this Tailored Infrastructure Section of Our Customer Terms, unless we agree otherwise, the following terms also apply:

(a) General Terms of Our Customer Terms (see http://www.telstra.com.au/customer-terms/business-government/index.htm); and

(b) General Terms of the Cloud Services section (see https://www.telstra.com.au/customer-terms/business-government#cloud-services); and

(c) other parts of the Cloud Services section, depending on the nature of the products and services that you receive from us.

1.2 For an explanation of the interrelationship between the various sections of Our Customer Terms see clause 1 of the General Terms of the Cloud Services section at the link above.

2 GENERAL

2.1 We do not monitor or manage any of your other services, including any of your other services provided under the Cloud Services section as part of your Tailored Infrastructure product.

2.2 Your options for configuring your Tailored Infrastructure products are set out on the Cloud Services portal at https://cloud.telstra.com/, or in your application form or Your Agreement.

2.3 You are responsible for ensuring that you comply with the licence terms of any software (such as application software or operating system) which you install or use in connection with your Tailored Infrastructure products.

2.4 You will be given a high degree of control over your Operating System configuration and management. If you configure and manage your Operating System in such a manner that causes disruption to your service and/or deletion of any of your data, you will be responsible for any loss that you suffer as a result and you may need to pay us an additional charge to fix any problems.

3 TAILORED INFRASTRUCTURE

3.1 Tailored Infrastructure (formerly Dedicated Hosting) provides you with dedicated infrastructure resources that are located in our Australian data centres and delivered as a service with offerings outlined in this section.

3.2 You may apply for one or more of the following Tailored Infrastructure offerings, each of which is a product:

(a) COMPUTE;

(i) Virtual Server (dedicated)

(ii) Managed Virtual Server (dedicated)

(iii) Managed Physical Server (dedicated)

(b) BACKUP & RECOVERY;

(i) Disaster Recovery (Gold)

(c) SOFTWARE.

3.3 If you cancel your Tailored Infrastructure product before the end of the minimum term set out in Your Agreement or we cancel your service as a result of your breach, we may charge you an early termination fee as set out in Your Agreement.

4 COMPUTE

4.1 You may apply for the following compute options:

(a) Virtual Server (dedicated)

(b) Managed Virtual Server (dedicated)

(c) Managed Physical Server (dedicated)

4.2 Prior to our execution of some service requests (including changes to your CPU and RAM configurations and restoration of storage snapshots) we may request that you power down the relevant server(s). We may be unable to address your service request until you have disabled the relevant server(s).

4.3 You need to nominate a system administrator to manage your servers and user access to the management console. You may request that we activate additional users or change existing user access privileges to the console.

4.4 If your service includes a Virtual Private Network (**VPN**) service, you will be responsible for loading and configuring any VPN software on your equipment.

4.5 We do not provide you with physical access to the server infrastructure.

4.6 We do not provide a facility for you to use accessories or peripheral devices with your server infrastructure, such as USB attachments or licence key dongles.

Software

4.7 From time to time we may make available different software services on the Cloud Services portal or via Your Agreement. The terms and conditions applicable to your use of the software are set out in Enterprise Software part of the Cloud Services section of Our Customer Terms at http://www.telstra.com.au/customer-terms/business-government/cloud-services/.

Operating Systems

4.8 The Operating Systems service includes a choice of pre-packaged operating systems for use with your shared or dedicated server(s).

4.9 If you have an existing licence to use one of the pre-packaged operating systems which are

set out in Your Agreement, you may use your existing operating system licence provided that you comply with the vendor software licensing terms and your operating system meets any compatibility requirements specified by us from time to time.

4.10 Where you provide your own operating system licence you are responsible for obtaining and maintaining an appropriate licence to use the operating system you provide on our service platform.

4.11 As set out in the table below, you may supply or request an operating system on shared or dedicated infrastructure in the following configurations.

Compute services	**Operating system Software media & License key(s)**	
	Shared	**Dedicated**
Virtual Server	Telstra supplied	Customer supplied
Managed Virtual Server	N/A	Telstra supplied or Customer supplied (License key only)
Managed Physical Server	N/A	Telstra supplied or Customer supplied (License key only)

Storage

4.12 The Storage service provides you with access to storage capacity on our service platform that can be used by you for various purposes including to store your data and applications.

4.13 Your Storage service includes:

(a) a data repository which may be partitioned into virtual disks for storing application, Operating System and file system data (you may request that we create additional disk partitions and we may charge you a fee); and

(b) levels of redundancy within our storage platform.

4.14 As part of the process for provisioning your Storage service, you may have existing data which you wish to migrate onto our storage platform. Refer to the Import and Export service below for further information.

4.15 Once a system disk has been created in your storage repository the storage capacity of the virtual disk cannot be decreased.

4.16 You are responsible for ensuring that all disks provided under the Storage service have sufficient free storage capacity in accordance with the system requirements for the relevant operating system you have selected.

Backup

4.17 The Backup service provides you with a facility to backup and restore your data on servers located in our managed data centres in the event of data corruption or failure.

4.18 The type and amount of data that will be backed up and the duration for frequency at which

it is kept will depend on your chosen configuration.

4.19 We will retain daily copies of file data and operating system data within the data repositories accessed by the servers and configured for backup for the retention periods set out Your Agreement.

4.20 We will not retain your backup data if you have terminated your service with us.

4.21 The Backup service backs up your operating system data and file data that is not otherwise being accessed at the time of the backup, in accordance with Your Agreement.

4.22 We may not be able to provide you with the Backup service if you make certain changes to your equipment or software. For this reason, we need you to tell us when you make changes that could affect the Backup service so that we can let you know whether your service is likely to be compromised. We cannot guarantee that backups created by the Backup service will be corruption or error free or capable of being restored.

4.23 The Backup service will create backup copies of the application data provided you have requested us to install the software plug-in for the application you wish to be backed up. If you do not request the installation of the appropriate software plug-in, the Backup service will create a data file backup of your application; however your Backup service will not create an application level backup of your application data.

4.24 If you require the Backup service to backup your structured application or database data, you are responsible for backing up such data in accordance with any instructions we set out in any relevant User Guides we provide.

4.25 In the event that a backup restoration is required, we will provide you with the backup files that you specify. You are responsible for the recovery of individual files from those backup files.

4.26 For Backup services acquired before 16 December 2013, the Backup service is designed for data sources where the average daily change rate in a week of backups per server is five percent or lower. If you applied for your Backup service on and from 8 April 2013 and your average daily change rate in a week is greater than five percent you may elect to pay an additional fee (which we will notify you of) or cancel your Backup service.

4.27 For Backup services acquired from 16 December 2013, the Backup service, the Backup service is designed to receive one percent or less of your data in each backup job. We may charge you an additional fee (which we will notify you of) for each job where more than one percent is received.

4.28 Notwithstanding any clause to the contrary in the General Terms of Our Customer Terms, we accept liability for loss of data in connection with your Backup service only where:

(a) that loss of data is directly attributable to our breach of contract or negligent act or omission; and

(b) the data lost is older than the last Recovery Point Objective (RPO) for your chosen Service Level Grade, as defined below.

The amount of any data loss for which we are liable is limited in aggregate to the total amount payable to us for your Cloud Services for 12 months of acquiring the relevant Cloud Services.

<u>Anti-Virus</u>

4.29 The Anti-Virus service provides a software based anti-virus capability. Terms applicable to this service are set out in the Security section below.

4.30 This service is available on the Managed Virtual Server (dedicated) and Managed Physical Server (dedicated) offerings.

Intrusion Prevention

4.31 The Intrusion Prevention service provides end-point software based intrusion detection capability. Terms applicable to this service are set out in the Security section below.

4.32 You must provide us with seven business days' notice before you undertake vulnerability or penetration testing of your network.

4.33 This service is available on the Managed Virtual Server (dedicated) and Managed Physical Server (dedicated) offerings.

VIRTUAL SERVER (DEDICATED)

4.34 This service provides you with a self-managed virtual server environment on your physical server infrastructure. You will have access to a hypervisor management toolset that provides limited access for the purposes of creating and managing your virtual servers.

4.35 You may use the hypervisor management toolset to create and configure virtual servers to which you may allocate CPU and RAM resources.

4.36 Your allocation of CPU and RAM resources to virtual servers may not exceed the total resource capacity purchased by you for your server infrastructure in accordance with Your Agreement.

4.37 In the event of an impact to your service through your use of the hypervisor management toolset, we will attempt to help you reinstate your service or recover your data but do not guarantee that we will be able to fully restore your service or data.

4.38 You are responsible for sourcing, installing and configuring all end-point security software which you wish to install on your virtual servers (including anti-virus and intrusion prevention software).

4.39 The hypervisor management toolset is a sophisticated tool and you are responsible for obtaining adequate training and certification in the use of the hypervisor management toolset we provide.

MANAGED VIRTUAL SERVER (DEDICATED)

4.40 This service provides you with a managed virtual server environment on your physical server infrastructure.

4.41 Your server management service includes:

(a) monitoring and management of the infrastructure allocated to you; and

(b) patch management with respect to the Operating System, Anti-Virus and Intrusion Protection services.

4.42 You may request that we create or reduce virtual servers on your behalf, subject to an additional charge.

4.43 You may request that we create or reduce the capacity of a virtual disk on your behalf, subject to an additional charge.

4.44 Your allocation of CPU and RAM resources to virtual servers may not exceed the total resource capacity purchased by you for your server infrastructure in accordance with Your Agreement.

4.45 You must notify us before you cause one of your virtual servers to restart or reboot or make any changes to the configuration of any applications running on your servers.

MANAGED PHYSICAL SERVER (DEDICATED)

4.46 This service provides dedicated infrastructure which is reserved for your use.

4.47 You may select from various base dedicated infrastructure configuration options in accordance with Your Agreement.

4.48 Your server management service includes:

(a) monitoring and management of the infrastructure allocated to you; and

(b) patch management with respect to the Operating System, Anti-Virus and Intrusion Protection services.

5 SERVICE LEVELS

5.1 The available service levels for Tailored Infrastructure are set out in the table below.

Service Level	Service Level Grade		
	Gold	Silver	Bronze
Service Support Coverage Hours	24 hours x 7 days		
Service Availability[1]	99.99%	99.95%	99.90%
Recovery Point Objective (RPO)	15 minutes	1 hour	24 hours
Recovery Time Objective (RTO)	45 minutes	2 hours	2 hours
Disaster Recovery	Disaster Recovery Gold (a fully operable duplicate system configuration located at a distant second site to the primary configuration is available as a failover target upon the primary's failure)	Disaster Recovery Silver (a duplicate system configuration located at a distant second site to the primary configuration which is only activated into operation as a failover target upon the primary's failure)	N/A
Service Activation			

Service Level	Service Level Grade		
	Gold	Silver	Bronze
Minor	5 business days[2]		
Standard	20 business days[2]		
Major	On Application		
Service Modification			
Pre-defined Modifications	as set out on the Cloud Services Management Console		
Projects	on application		
Incident Response Time			
Severity 1	15 minutes		
Severity 2	30 minutes		
Severity 3	45 minutes[3]		
Severity 4	120 minutes[3]		
Incident Restore Time			
Severity 1	2 hours		
Severity 2	6 hours		
Severity 3	8 hours[3]		
Severity 4	24 hours[3]		

[1] Service Availability is calculated each month and measured on the preceding 12 months in accordance with Table 3 below.

[2] Provided that the request is logged before 1pm on a business day. If the request is logged after 1pm, measurement of Service Activation or Service Modification commences at 9am on the following business day.

[3] We only accept responsibility for a failure to meet this service level if the incident relating to the relevant product occurs between 7am and 7pm on a business day.

Service Level Exclusions

5.2 In addition to the service level exclusions in the General Terms for Cloud Services, we are not responsible for a failure to meet a service level where:

(a) the failure is caused due to the corruption of data as part of a backup;

(b) your failure to comply with a request from us to maintain sufficient storage capacity for your virtual disks provided under your Storage feature under the Infrastructure part of the Cloud Services section;

(c) the failure relates to your operation of an application on our service platform, as part of a service under the Cloud Services section, which is not version "n-1" or later; or

(d) the failure occurs in relation to your Management service under your Infrastructure Hosting product under the Data Centres part within the first two months of receiving this service (during which we undertake testing and improvement activities in relation to the Cabinet service).

Service Level Rebates

5.3 If we fail to meet the Service Availability service level set out in the table above for your Tailored Infrastructure service, you may apply for a rebate in accordance with this clause.

5.4 If:

(a) your service is unavailable due to a problem caused by us and outside any nominated Telstra service window; and

(b) the actual Service Availability of your service is below that allowed under the Service Availability service level which corresponds to your product,

then in each monthly period in which the actual Service Availability is below the allowed Service Availability for your service, you may apply for a rebate of five percent (5%) of your monthly service fee for each 30 minute block of unavailability exceeding the threshold contemplated under paragraph (b) above, to a maximum of 100% of your monthly service fee.

5.5 Any rebate will be applied to your Telstra bill (at the end of the billing cycle).

6 ADDITIONAL SERVICES

6.1 You can apply for the following additional services in connection with your Tailored Infrastructure product:

(a) Disaster Recovery;

(b) Public Network;

(c) Private Network;

(d) Security; and

(e) Data Import and Data Export.

7 DISASTER RECOVERY

7.1 You may apply for the following backup and recovery services.

(a) Disaster Recovery (Gold)

7.2 We do not provide you with physical access to the backup and recovery infrastructure.

Disaster Recovery

7.3 The Disaster Recovery service provides you with recovery of your cloud services in the event of a disaster in accordance with agreed service levels (depending on your chosen Service Level Grade).

7.4 You may apply for one or more of the following disaster recovery services:

(a) Disaster Recovery (Gold).

7.5 The Disaster Recovery (Gold) service is available with the following Compute services:

(a) Managed Virtual Server (Dedicated)

(b) Managed Physical Server (Dedicated)

7.6 If you cancel your Compute service, your corresponding Disaster Recovery service will also be cancelled.

7.7 If you select a Gold Service Level Grade for your Compute service, you must also acquire Disaster Recovery (Gold) otherwise we are not liable for any failure to meet the Service Level Targets.

7.8 For the purposes of this service, a disaster means the occurrence of any one or more of the following events:

(a) loss of one or more business critical systems (you must nominate which business systems are critical prior to activation of your service); or

(b) loss of service or unplanned outage.

a disaster does not include:

(c) a planned outage; or

(d) planned upgrades or works,

to your hosting or network services.

7.9 If a disaster occurs and once you have confirmed activation of your disaster recovery plan, we will aim to recover your services within the Recovery Time Objective up to the Recovery Point Objective (as defined in the service levels section of the General Terms part of the Cloud Services section).

7.10 For the purposes of this service, 'recovery' means:

(a) restoration of your critical business services;

(b) a full recovery with all systems at full capacity; or

(c) a partial recovery with only core systems and limited functionality.

Recovery and restoration will be as defined in your disaster recovery plan or business continuity plan ('disaster recovery documentation').

7.11 The Disaster Recovery service does not include us providing you with disaster recovery documentation. We may be able to provide you with assistance in preparing your disaster recovery documentation for an additional fee.

7.12 You are responsible for ensuring that your disaster recovery documentation and policies are kept up to date. You must provide us with scripts, policies and all relevant information for us to provide the service.

7.13 Following any service modification to your dedicated servers for which you also have Disaster

Recovery (Gold), up to 10 business days is required to assess the impact of the service modification on your Disaster Recovery (Gold) service and re-implement your Disaster Recovery (Gold) settings, if required. During this period service levels and RTO's are suspended.

8 PUBLIC NETWORK SERVICES

Internet

8.1 Internet connectivity is included as a feature of your Tailored Infrastructure product. The service level for your internet connectivity is the same as the Tailored Infrastructure product. Usage charges for internet connectivity are set out in Your Agreement.

Load Balancing

8.2 You can apply for the following load balancing services:

Service	Public Network	Private Network
Server Load Balancing	✓	✓
SSL Offloading	✓	✓
Geographic Server Load Balancing	✓^	N/A

^ *between Sydney and Melbourne data centres only*

Server Load Balancing

8.3 Server Load Balancing provides a full proxy between users and application servers that creates a layer of abstraction to help secure, optimise, and load-balance traffic.

SSL Offloading

8.4 This service provides secure sockets layer (SSL) offloading for your Public Network product.

8.5 SSL Offloading is only available with Server Load Balancing.

Geographic Server Load Balancing

8.6 Geographic Server Load Balancing provides users an enhanced implementation of DNS to spread workload across multiple sites.

Domain Name Registration

8.7 We offer a domain name registration service. If you ask us to register or renew a domain name on your behalf as part of your service (and we agree to do this for you), these terms apply to you.

8.8 The Domain Name Registration service includes us registering a domain name on your behalf and assisting you with communicating with the relevant registrar of the domain name, where necessary. You acknowledge that we can only register a domain name on your behalf if that domain name is available for use.

8.9 If you request us to register a .com, .net, .org, .biz, or .info domain name ("**TLDs**" or "**Top**

Level Domains") on your behalf, the General Registrar Policy located at http://www.tppinternet.com.au/terms-conditions/australian_domains.php is incorporated into this agreement as amended from time to time.

8.10 If you request that we register a .au domain name on your behalf, the policies applicable to .au Domain Name Licences located at http://www.tppinternet.com.au/terms-conditions/gtld-domain-names.php, as amended from time to time and the .au 2LD Domain Name Eligibility and Allocation Policy Rules issued located at https://www.auda.org.au/policies/, as amended from time to time are incorporated into this agreement.

8.11 You acknowledge that additional policies relating to your domain name may come into effect from time to time and you agree to comply with such additional policies.

8.12 If there is a dispute regarding the registration or use of your TLD, you agree to:

(a) submit to and be bound by Uniform Domain Name Dispute Resolution Policy located at http://www.icann.org/udrp/udrp.htm as amended from time to time; and

(b) be subject to arbitration, suspension or cancellation by any ICANN procedure, or by any registry administrator procedure approved by ICANN policy, relating to:

(i) the correction of mistakes by us or the registry administrator in registering the domain name; or

(ii) the resolution of disputes concerning the domain name.

8.13 In the event of a dispute in registering a .au Domain, or a dispute about a .au Domain after registration, you will submit to and be bound by the .au Dispute Resolution Policy (auDRP) located at https://www.auda.org.au/policies/, as amended from time to time.

8.14 You must pay any registration or delegation charges to us in advance. We cannot register a domain name for you unless you pay for it in advance.

8.15 You authorise and direct us to nominate Telstra Corporation Limited (ABN 33 051 775 556) as the authorised billing contact for your domain name.

8.16 We are not liable for any loss or damage resulting from the non-renewal of your domain name if you fail to provide us with consent to renew the domain name registration or you delay in providing us with such consent.

8.17 You indemnify us against all claims arising out of the registration, use or renewal of your domain name, unless and to the extent that the claim arises out of our breach of this agreement, or our negligent act or omission.

SMTP Mail Relay

8.18 The SMTP Mail Relay service for the Public Network product provides you with a dedicated mail relay for use with any mail servers that you operate on our service platform.

DOS & DDOS Protection of Telstra Cloud Services

8.19 In the event of a DOS or DDOS attack directed against a customer service hosted by Telstra we reserve the right to take any reasonable steps to protect the hosting compute platform. Unless you are able to activate an effective DOS or DDOS mitigation strategy this may involve *rate limiting* traffic and/or *blacklisting* the source IP addresses or *black-holing* the affected service (removing it from service).

9 PRIVATE NETWORK SERVICES

Next IP services

9.1 Next IP connectivity is included as a feature of your Tailored Infrastructure product. The service level for your Next IP connectivity is the same as your Tailored Infrastructure product. Usage charges for Next IP connectivity are set out in Your Agreement.

SMTP Mail Relay

9.2 The SMTP Mail Relay service for the Private Network product provides you with a dedicated mail relay for use with any mail servers that you operate on our service platform.

10 SECURITY SERVICES – DEDICATED GATEWAY

Cease sale and exit notification

10.1 Dedicated Gateway is not available for purchase by new customers from 1 April 2021.

10.2 Existing customers may continue to receive Dedicated Gateway, but from 30 November 2021 will no longer be able to add new services, make changes to existing services or recontract existing services although will still be able to make policy changes.

10.3 Dedicated Gateway will no longer be available to existing customers from 31 May 2022.

What is Dedicated Gateway?

10.4 Dedicated Gateway (formerly Security Premium) a hosted security gateway located in our Tailored Infrastructure data centres.

10.5 You may apply for one or more of the following security services as part of your Dedicated Gateway:

Service	Public Network	Private Network
Internet Protection Services	✓	N/A
Denial of Service Protection	✓	N/A
Firewall (Dedicated)	✓	✓
Firewall (Shared)	✓	✓
Intrusion Prevention (Dedicated)^	N/A	N/A
Intrusion Prevention (Shared)	✓	✓
IPSEC VPN	✓	N/A
SSL VPN	✓	N/A
Vulnerability Discovery	✓	✓

^ Intrusion Prevention (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.

Internet Protection Services

10.6 The Internet Protection Services provides security features for email and/or web traffic across your network.

10.7 The terms and conditions for the Internet Protection Services are set out in Part D (Internet Protection Services) of the Internet Solutions section at http://www.telstra.com.au/customer-terms/business-government/internet-services/internet-solutions/.

Denial of Service Protection

10.8 The Denial of Service Protection service is designed to filter certain network traffic in our network to assist you in managing the potential impact of distributed denial of service and other agreed attacks which may impact your Internet data service. The Denial of Service Protection service does this by comparing network traffic flows to your Data service based on agreed profiles of normal traffic patterns, behaviour and protocol compliance.

10.9 We do not guarantee that the Denial of Service Protection service will prevent all attacks against your Internet data service. In particular, the service may not provide any protection or assistance to you arising out of an attack to your Internet data service if:

(a) the distributed attack is an application level attack that is not detectable from traffic flows and not threatening the capacity of your Data service; or

(b) the attack occurs during the four week period immediately following the activation of the Service as the Service is adapting to the appropriate network traffic profiles during this period.

10.10 The Denial of Service Protection service is designed to limit network traffic to the Internet data service. If the service detects an attack, then you acknowledge and agree that:

(a) certain network traffic may be blocked from reaching the Internet data service or discarded in our network; and

(b) your use of the Internet data service may be degraded due to network congestion or other related effects.

10.11 You acknowledge that if data traffic volumes from attacks being mitigated by the Denial of Service Protection service exceed or are expected to exceed the capacity of the Denial of Service Protection service then, in order to maintain availability for the majority of your users, further filtering of attack traffic may be implemented at peering points and by network providers carrying traffic before it reaches our networks and this filtering may increase the level of legitimate traffic blocked.

10.12 We are not responsible for any loss that you suffer as a result of the Denial of Service Protection service blocking or limiting Data traffic due to an attack.

Firewall

10.13 The Firewall service is a security service which is designed to provide you with functionality to assist you in restricting certain access and traffic into your network.

10.14 The Firewall service provides the following features as selected by you in accordance with your application form or other agreement with us, the availability of which may depend on the firewall tier which you select:

(a) back-up of your configuration data;

(b) reporting of traffic volumes, user activity and device performance;.

(c) an ability to make policy or configuration changes;

(d) data retention / Storage (Logs Files);

(e) a quarterly vulnerability assessment (only for customers who acquired their service before 31 May 2012);

(f) site to site VPN connections (depending on your platform selection);

(g) client to site VPN support;

(h) security event monitoring; and

(i) threat analysis and intelligence service.

10.15 Under the shared firewall configuration, the features of your service will depend on the service tier that you select.

10.16 Under the dedicated firewall configuration, the hardware that we use to provide you with the service will be dedicated to you and the services of your service will depend on the service tier that you select.

10.17 The dedicated firewall configuration also includes:

(a) custom analysis, design and configuration of your dedicated firewalls;

(b) management of change requests to your Firewall service; and

(c) access to any additional firewall modules (such as a deep packet inspection module) where these modules are supported by your chosen firewall.

10.18 We do not promise that the Firewall service will prevent unauthorised access to your network.

10.19 We can only provide the Firewall service for the devices that are managed by us.

10.20 If you select a dedicated firewall service, we do not guarantee that the additional modules will remove all viruses or correctly identify all viruses, screen or block all spam or correctly identify all spam, block all websites you ask us to block or correctly identify websites that you have requested to be blocked or block all network activity you ask us to block or correctly detect network activity that you deem suspicious.

Intrusion Prevention (Network)

10.21 This service provides intrusion protection for the public and private networks and comprises:

(a) attack recognition and response service;

(b) notification to you if we become aware of a security threat;

(c) automatic escalation process for known threats and vulnerabilities; and

(d) monitoring of traffic and uptime when an unauthorised intrusion has occurred.

10.22 We cannot guarantee that the Intrusion Protection service will protect against all attacks

SSL VPN/IPSEC VPN

10.23 IPSEC VPN allows you to access your shared or dedicated servers over the Public Network via your Dedicated Gateway service using IPSEC tunnelling technology

10.24 SSL VPN allows you to access your shared or dedicated servers over the Public Network via your Dedicated Gateway service using SSL tunnelling technology.

10.25 We do not promise that the SSL/IPSEC VPN service will prevent or detect all unauthorised access to your network.

Vulnerability Discovery

10.26 The Vulnerability Discovery service provides vulnerability assessments and includes proactive scanning of your network from within to identify and prioritise potential weak points, risk areas and security exposures. As part of your Vulnerability Discovery service we will provide a Vulnerability Discovery report which will set out:

(a) the date of the Vulnerability Discovery scan;

(b) the scope of the Vulnerability Discovery scan;

(c) an inventory of hosts, operating systems and applications;

(d) a list of vulnerable hosts;

(e) the types of vulnerability detected; and

(f) an explanation of the risk for vulnerabilities detected.

11 DATA IMPORT AND DATA EXPORT

General

11.1 The Data Import and Data Export service enables you to transfer your data to and from your Infrastructure products via a physical storage device ("Device").

11.2 The Data Import and Export services will usually be performed during business hours. An additional charge may apply if you request Data Import or Export services outside business hours.

11.3 You must comply with the instructions we provide to you in connection with the transfer of your data.

11.4 If we supply you with a Device and you have not returned the Device to us within one month of receipt, we may charge you for the replacement cost of the Device (as set out in Your Agreement).

Data Import

11.5 Upon application, we will provide you with a Device for you to transfer your data onto and return to us.

11.6 Following receipt of the Device, we will notify you once we have connected the Device to your chosen service and you can then transfer the data to the appropriate server(s).

Data Export

11.7 You will provide us with a Device for us to transfer your data onto and return to you. The Device must be blank and sufficient to hold the quantity of data you require transferred. Alternatively we can supply a Device, the charges for which are set out in Your Agreement.

11.8 Following receipt of the Device, we will connect the Device to your chosen service and we will then copy the data from the appropriate server(s) to the Device.

11.9 Once we have copied the data from the server(s) to the Device, we will notify you that the Device is ready for collection. Alternatively, upon request, we will return the Device to you via our nominated courier.

11.10 We will retain the data on your server(s) until such time as you either:

(a) cancel your Cloud Services product; or

(b) request that we delete the data,

following which we will securely delete the data. Please note that the charges for your Cloud Services product will continue to apply until such time as the Cloud Services product is cancelled.

Liability

11.11 Unless you supply your own Device, we retain title to the Device at all times. Risk of loss or damage to the Device and any data stored on it is with you whilst in transit. You may wish to insure the Device and data whilst in transit. If the Device is lost, stolen or damaged, we may charge you for a replacement Device (unless you have supplied your own Device).

11.12 You are responsible for protecting your data on the Device. We strongly recommend that you encrypt your data in accordance with the instructions we provide with the Device.

11.13 We are not responsible for any loss, theft or damage to the Device or your data other than as a direct consequence of our negligence.

11.14 You are responsible for ensuring that you comply with all applicable laws and have all necessary rights to provide the data to us for transfer onto your server(s). You acknowledge we may need to reproduce the data to transfer it between the Device and your server(s).

12 WHAT IS HYBRID DISASTER RECOVERY?

12.1 Hybrid Disaster Recovery is a self-managed, software solution that enables the recovery of your chosen services in the event of a 'disaster' (as defined below). The Hybrid Disaster Recovery service supports failover between your premises or a third party facility and Telstra Cloud and Tailored Infrastructure (dedicated) services, as well as between Telstra Cloud and Tailored Infrastructure (dedicated) services.

12.2 Your production environment located at your premises, a third party facility, Telstra Cloud Infrastructure (dedicated) or Tailored Infrastructure (dedicated) service which you wish to failover in the event of a disaster is referred to as your 'primary environment' in this Hybrid Disaster Recovery part. The Telstra Cloud Infrastructure (dedicated) or Tailored Infrastructure (dedicated) service which you wish your primary environment to failover to is referred to as your 'recovery environment' in this Hybrid Disaster Recovery part.

12.3 You are responsible for installing the Hybrid Disaster Recovery software and the creation of your disaster recovery plan. We will provide you with a Hybrid Disaster Recovery User Guide to explain how to install the Hybrid Disaster Recovery software. Support for the Hybrid Disaster Recovery service is limited to issues with the Hybrid Disaster Recovery software not working correctly. You can install and manage your Hybrid Disaster Recovery service via the Cloud Services management console.

12.4 You acknowledge that some personal information may be accessed, in accordance with our privacy policy, from overseas via our contractors or suppliers for the purposes of providing support for your Hybrid Disaster Recovery service.

Eligibility

12.5 The Hybrid Disaster Recovery service is only available to new or existing Cloud Services customers in Australia.

12.6 To acquire the Hybrid Disaster Recovery service you must have:

(a) one or more primary and/or recovery environment(s) on:

(i) Cloud Infrastructure - Virtual Server (Dedicated);

(ii) Tailored Infrastructure - Virtual Server (Dedicated);

(each a "Compute" service)

(b) a compatible hypervisor installed on your servers. Details of compatible hypervisors are set out in the Hybrid Disaster Recovery User Guide;

(c) depending on the size of your primary environment, at least one clear server in your primary environment onto which you can install the Virtual Server Agent for VMware, and at least one clear server in your recovery environment onto which you'll install both the Virtual Server Agent and the Media Agent software. For further information on the space needed for the Virtual Server Agent and Media Agent, please refer to the Hybrid Disaster Recovery User Guide; and

(d) enough storage in your recovery environment.

12.7 If you cancel your Compute service, your corresponding Hybrid Disaster Recovery service will also be cancelled.

Invoking failover

12.8 If a disaster occurs and you have an active Hybrid Disaster Recovery service, you will be responsible for invoking the fail over and restoration of your services within the Cloud Services management console. The Recovery Time Objective and Recovery Point Objective are target services levels (as defined in the service levels section below).

12.9 For the purposes of this Hybrid Disaster Recovery service, a 'disaster' means the occurrence

of any one or more of the following events:

(a) loss of one or more business critical systems (you must nominate which business systems are critical prior to activation of your service); or

(b) loss of service or unplanned outage.

a disaster does not include:

(c) a planned outage; or

(d) planned upgrades or works,

to your hosting or network services.

12.10 For the purposes of this service, 'recovery' means:

(a) restoration of your critical business services;

(b) a full recovery with all systems at full capacity; or

(c) a partial recovery with only core systems and limited functionality.

12.11 The Hybrid Disaster Recovery service does not include us providing you with disaster recovery documentation. We may be able to provide you with assistance in preparing your disaster recovery documentation for an additional fee.

Your obligations

12.12 You are responsible for ensuring that your disaster recovery plan and policies are kept up to date.

12.13 You are responsible for testing the service to ensure that failover and restoration works successfully.

12.14 You must keep confidential and not disclose any software licence keys to which you have access to in connection with the Hybrid Disaster Recovery service.

Charges

12.15 The charges for your Hybrid Disaster Recovery service are set out on the Cloud Services Management Console or Your Agreement.

12.16 Charges for your Hybrid Disaster Recovery service are calculated each month based on the maximum number of virtual machines in your [primary and recovery] environment within your Hybrid Disaster Recovery service in that month.

For example if you have 50 virtual machines within your Hybrid Disaster Recovery service and add an additional 20 virtual machines during the month, you will be charged for 70 virtual machines for that month.

12.17 The charges for your Hybrid Disaster Recovery service are only for the Hybrid Disaster Recovery software and do not include any infrastructure resources (such as compute, storage and network) used in connection with your primary or recovery environments.

Hybrid Disaster Recovery Software

12.18 In addition to the clauses relating to service software in the General Terms part of the Cloud

Services section, the following terms apply to your and your end users' use of the software included in your Hybrid Disaster Recovery service.

12.19 The Hybrid Disaster Recovery service software comprises CommVault Simpana as well as Microsoft SQL Server software and other third party software (together the "Software").

12.20 You may use the Software in numbers equal to the number of licenses purchased.

12.21 All title and intellectual property rights in and to the Software are owned by Telstra and/or its licensors (for example CommVault and Microsoft). Such licensors, in addition to any other rights or remedies available to them, are third party beneficiaries of the terms set out in this section 0 for their respective software and may have the right to enforce such terms against you.

12.22 You agree to use the Software solely for your internal data centre operations and to restrict any access to the Software, documentation, or other user information accompanying the Software only to those of your employees having a need to have such access for your internal data processing operations.

12.23 The export of the Software may be restricted by the export control laws of the United States of America and other countries. You agree to comply strictly with all such regulations and acknowledge that you have the responsibility to obtain licenses to export, re-export, or import Software.

12.24 To ensure compliance with this section 0, you agree that upon reasonable notice, we or our authorised representative will have the right to inspect and audit your installation and use of the Software. Any such inspection or audit shall be conducted during regular business hours at your facilities or electronically. Any information obtained during the course of such audit will be used by us solely for the enforcement of our rights under this section 0 and applicable law. If such audits disclose that you have installed, accessed, used, or otherwise permitted access to the Software in a manner that is not permitted by the terms of this section 0 and after receiving notice of such breach you still remain in default, then we may terminate your Hybrid Disaster Recovery service You will pay for any unpaid license fees and all reasonable expenses related to such audit.

12.25 You acknowledge and agree that the Software may automatically provide certain reports and survey information regarding its use to us. You may disable this reporting feature at any time. Any such reports or information shall be kept confidential and used solely by us or our licensors for internal purposes and/or in a manner that does not identify you.

12.26 The Software may contain support for programs written in java. Java technology is not fault tolerant and is not designed, manufactured, or intended for use or resale as online control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of java technology could lead directly to death, personal injury or severe physical or environmental damage.

12.27 The Software may contain certain software licensed by Microsoft. You acknowledge that you are not licensing Microsoft products under this EULA and that any copies of Microsoft software that you receive as a result of licensing the Software do not entitle you to maintain on your computer systems any more copies of Microsoft software than you may have previously licensed from Microsoft or other third parties.

Service Levels

12.28 Unless a service level exclusion applies, we aim to meet the service levels in this section for your Hybrid Disaster Recovery service. You acknowledge that the service levels are targets only and we will not be responsible for failing to meet them.

Table 1 – Description of Service Levels

Service Level	
Service Support Coverage Hours	24 hours x 7 days
Recovery Point Objective (RPO)	2 hours
Recovery Time Objective (RTO)	2 hours
Service Activation	
Self Installation	
Incident Response Time	
Severity 1	15 minutes
Severity 2	30 minutes
Severity 3	45 minutes[1]
Severity 4	120 minutes[1]
Incident Restore Time	
Severity 1	24 hours
Severity 2	72 hours
Severity 3	20 days
Severity 4	N/A

[1] We only accept responsibility for a failure to meet this service level if the incident relating to the relevant product occurs between 7am and 7pm on a business day.

Service Level Exclusions

12.29 In addition to the service level exclusions in the General Terms for Cloud Services, we are not responsible for a failure to meet a service level where:

(a) you fail to follow our documented instructions in the Hybrid Disaster Recovery User Guide for installing the Hybrid Disaster Recovery software or follow the steps required to restore your services to the secondary infrastructure site;

(b) if you fail to have your recovery environment on either a Telstra Cloud Infrastructure (dedicated) or Tailored Infrastructure (dedicated) service;

(c) the failure is caused due to the corruption of data as part of a backup;

(d) you fail to comply with a request from us to maintain sufficient storage capacity for your virtual disks provided under your Storage feature under the Infrastructure part of the Cloud Services section;

(e) the failure relates to your operation of an application on our service platform, as part of a service under the Cloud Services section, which is not version "n-1" or later; or

Outages

12.30 In addition to the outages described in the General Terms for Cloud Services, we will endeavour to carry out scheduled maintenance when we need to implement upgrades to the Hybrid Disaster Recovery software version without affecting your products, services or features. However, your products, services or features may not be available during these periods.