Public Cloud Connect

Service Terms

Version 1.0

28th Sep 2016

Table of Contents

1. Introduction

1.1 This section defines the Service Terms of the Public Cloud Connect product provided by Telarus to the Customers. This document forms part of our Standard Form of Agreement (SOFA), which includes the following:

(a) General Terms and Conditions
(b) Service Terms

2. Definitions

- **"Customer"** means a natural person or registered commercial entity that has entered into a commercial relationship with Telarus for the purpose of procuring services as identified upon a Service Order. Hereinafter it is referred to as "Customer", "you", "your".
- **"Customer Data"** means all data or intellectual property which is owned by Customer and transferred into the Telarus environment for the purpose of using Telarus Service.
- **"Customer Nominated Contact"** means an email and telephone contact detail of an authorized customer representative, supplied to Telarus for the purpose of formal communication. (including system integrators)
- **"Customer Notice"** means a communication in written electronic form, delivered via Electronic Mail (email) to the Customer nominated contact followed by an elapsed period of four hours.
- **"DMZ"** refers to the Demilitarized Zone: a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network (e.g.: Internet).
- **"Force majeure"** means an event or circumstance beyond the reasonable control of Telarus.
- **"Information Form"** means a form required for Customer to fill in whenever starting Telarus Public Cloud Connect service or change the service. It includes all information that Telarus need to connect Customer to the public cloud.
- **"Minimum contract period"** means the period specified in your Service Order that starts from the Service Commencement Date.
- **"MPLS VPN"** is a family of methods for using multiprotocol label switching (MPLS) to create virtual private networks (VPNs). MPLS VPN is a flexible method to transport and route several types of network traffic using an MPLS backbone.
- **"Nominal bandwidth"** means the bandwidth specified in your Service Order, the theoretical maximum bandwidth.
- **"Scheduled Maintenance"** means a planned activity performed with customer notice and having a minimum notice period.

- **"Service Cancellation Date"** means the calendar date upon which Telarus has provisioned and starts to provide the service identified upon a Service Order.
- **"Service Commencement Date"** means the calendar date upon which Telarus will cease to provide the service identified upon a Service Order.
- **"Service Level"** means the percentage of time within a calendar month when the service is available to the Customer.
- **"Service Level Rebate"** means the available refund to Customer for a service due to specific duration of service outage.
- **"Telarus"** means Telarus Pty Ltd ABN 56 099 202 721 Level 8, 473 Bourke Street, Melbourne, Victoria trading as Telarus. Hereinafter it is referred to as "Telarus", "we", "us", "our".
- **"TMS"** refers to Telarus Managed Security, a centralised solution applied at the public gateway to protect customer sites and resources on their managed private network from external security threats.
- **"Unavailability"** means a service resource is failing to perform within a tolerance of 20% of its defined operating parameters. See Clause 11.3 for details.

3. Public Cloud Connect Offerings and Service

3.1 Telarus Public Cloud Connect service provides customers with managed private connectivity with public cloud vendor Amazon AWS and Microsoft (Azure and Office 365). It provides customers with multiple options for the connection bandwidth starting from 10M (for AWS) or 50M (for Microsoft).

3.2 There are three modes for customer's connection to the public cloud AWS:

(a) Private connection: Customer will connect to the public cloud directly via their MPLS VPN;

(b) Securely-managed connection: Connection to the public cloud will go through a DMZ port of TMS firewall instance. Customer will need to order Telarus TMS product to manage the secure connection to the public cloud;

(c) Hybrid connection: a mixture of the above. Customer traffic which needs high level of protection will go through a DMZ port of TMS firewall instance, while other Customer traffic is directly connected to the public cloud.

3.3 There are three routing domains for customer's connection to the public cloud Azure and Office 365:

(a) Private domain: Azure virtual machine and cloud services, customer may connect directly via their MPLS VPN;

(b) Public domain: Azure storage, SQL and website service, customer must connect through a DMZ port of TMS firewall instance. Customer will need to order Telarus TMS product to manage the secure connection to the public cloud;

(c) Microsoft domain: Microsoft online service including Office 365, customer must connect through a DMZ port of TMS firewall instance. Customer will need to order Telarus TMS product to manage the secure connection to the public cloud.

Customer can choose to have up to three domains in their Azure ExpressRoute.

4. Contract and Payment

4.1 The following Public Cloud Connect services do not have a minimum contract term. Customers can choose to have a month-by-month service, or a contract of 12/24/36 months with reduced setup fees.

(a) Private mode of AWS connection;
(b) Azure connection in which customers only select the private domain.

4.2 For other modes or types of Telarus Public Cloud Connect services, the minimum contract term will be the same as Telarus TMS product. See Telarus TMS business terms for details.

4.3 Payment for the Public Cloud Connect service is required to be conducted monthly in advance. Customers are required to pay for the service monthly.

5. Billing

5.1 Billing is issued monthly in advance at the beginning of each calendar month.

5.2 Customer adjustment of service are billed monthly in arrears.

5.3 Invoice will be delivered electronically to Customer Nominated Contact.

6. Security

6.1 For the private/hybrid modes of AWS Cloud Connect service, and the private domain of Azure Cloud Connect service:

(a) You will be responsible for implementing and maintained network security at your site, appropriate security measures need to be taken by you.
(b) Telarus will not be responsible for any security-related issues regarding Customer traffic via direct connection to the Public Cloud and Customer data in the MPLS network.
(c) The transmitted data on the link from and to public cloud is at customer's own risk.

(d) Should the customer fail to implement security measures on the connection and result in a security breach or compromise, Telarus reserve the right to suspend the Public Cloud Connect service and send Customer notice as soon as practicable to the Customer nominated contact, requiring Customer to rectify. This includes but not limits to the following:
    (i) Evidence of hacker activity;
    (ii) Virus, malware, or other malicious code;
    (iii) Spamming which jeopardizes our operation or the service provided to other Customers.
(e) If the security breach is not rectified by the Customer within a reasonable timeframe, Telarus may terminate the Public Cloud Connect service of the specific Customer and reserves the right to refuse refund on Customer service.
(f) For the hybrid modes of AWS Cloud Connect service, Telarus TMS will protect Customer data on the best-effort basis which goes through the DMZ port as a secure channel, see Telarus TMS Service Terms for details.

6.2 For the securely-managed mode of AWS Cloud Connect service and the public/Microsoft domains of Azure Cloud Connect service:
(a) Telarus TMS product will be responsible for the protection of the link between the Customer MPLS network and the public cloud.
(b) Telarus protection of customer data will be on the best-effort basis. See Clause 12 of Telarus TMS Service Terms for details.
(c) The protection inside Customer managed private network (MPLS) still needs to be managed by the Customer's self-managed security solution and Telarus takes no responsibility for risks and attacks from traffic within the managed private network.

6.3 Telarus assumes that any access to the Public Cloud Connect service is authorized by the customer. You are responsible for preventing any unintended access to your service. Customers will still be charged for usages of services if the service is used by a third party.

7. Service Provisioning

7.1 For existing Customer who has managed network service with Telarus, the standard provisioning period for Telarus Public Cloud Connect service is 5 business days.

7.2 Telarus Public Cloud Connect service is only available for Customers who have managed network service (MPLS) at Telarus. New Customers need to be set up in Telarus managed network to be available for the Public Cloud Connect service. See corresponding Telarus Service Terms for the provisioning period of specific service to connect to Telarus managed network.

7.3 For hybrid/securely-managed modes of AWS Cloud Connect and public/Microsoft domains of Azure Cloud Connect, customers also need to go through the design phase with Telarus before the public cloud connection can be set up. See Clause 10 of Telarus TMS Service Terms for details.

7.4 For new Customers who do not have a managed network service with Telarus, we will nominate a detailed provisioning timeframe upon each service order.

7.5 Customers need to provide required information correctly regarding the public cloud in the Information Form after the service order is accepted. Telarus cannot start provisioning if the information is found to be incorrect.

7.6 For Azure or Office 365 connection, you need to provide us a valid Azure ExpressRoute service key before we start the provisioning process.

7.7 Telarus reserve the right to withdraw the service from the market after a 15 calendar days' notice to Customers.

8. Service Changes

8.1 You can change the bandwidth for your connection to public cloud at any time. For customers with hybrid offerings for AWS or multiple domains for Azure, you can nominate the bandwidth allocation for secure and direct links at any time.

8.2 Upon each request for bandwidth change, Customer needs to fill in the Information Form with correct information. Telarus will implement the change request within 5 business days if we verify the information is correct.

8.3 For Customers under hybrid/securely-managed offerings for AWS, or include Public/Microsoft domains for Azure, their connection bandwidths to the public cloud via the secure link cannot exceed their applied bandwidths of TMS product. Customer needs to upgrade their bandwidth in TMS before they can get a high bandwidth via secure link to the public cloud.

8.4 For any early termination or cancellation of the Public Cloud Connect service:

(a) For a month-to-month service, Customer must pay in full of all outstanding balance in the calendar month when Telarus approve their request.

(b) For Customers with fixed-length contract, see Clause 12 and 75 of Telarus Business Terms for details.

9. Demarcation

9.1 The nominal upload and download bandwidths are theoretical maximum only, and may not be achievable in practice. This is because the transmission protocol uses some of the access bandwidth to manage the data transmission. There may be variations in performance times and capacity of the service.

9.2 The demarcation point for Telarus Public Cloud Connect service is the virtual gateway to attach to the public cloud. Telarus will not be responsible for any issues in the public cloud supplier domain.

9.3 Telarus is not responsible for any issues relating to Customer data, usage, or operation within the public cloud.

9.4 Telarus is not responsible for any loss, theft or damage to customer device or data other than as a direct consequence of our negligence.

10. Data Retention

10.1 Telarus may keep the meta data relating to Public Cloud Connect service for an indefinite period of time, according to **Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015**. This includes but is not limited to the following:

(a) Customer account data and contact information
(b) Customer contract information
(c) Payment and billing information
(d) Service usage

11. Service Levels and Rebates

11.1 Telarus provides a Service Level Target of 99.9% for Public Cloud Connect service.

11.2 The Service Level Availability (SLA) represents the percentage of time Telarus Public Cloud Connect service is expected to be available during calendar month. It is calculated as: (Service hours – Unavailable hours) / Service Hours * 100%. Telarus is only responsible for the guarantee of SLA on the connection that is provided and managed by Telarus.

11.3 Service unavailability is when a network path is considered to be inaccessible if either:

(a) Network traffic fails to pass permitted communications for a period in excess of 5 minutes;

(b) The performance of the service is severely degraded to an extent that the service is effectively unavailable. Severe degradation occurs where in excess of 20% of the packets transmitted on the path are lost during a period of 15 minutes.

11.4 The following activities by Telarus will be excluded from the calculation of Service Hours:

(c) Scheduled Maintenance or planned outage. E.g.: software upgrade.
(d) Remediation activities to provide a safe work environment
(e) Unavailability caused by force majeure
(f) Unavailability caused by suspension or termination of service as required by law or as otherwise permitted in the Telarus Business Terms
(g) Unavailability caused by maintenance from Customer request

11.5 The following service rebate applies when the service level availability falls below a certain level for each discrete service resource:

Service Unavailability in any month	% Rebate of Monthly Recurring Charge
Less than 1 hour	Not Available
More than 1 hour but less than 4 hours	15%
More than 4 hours	30%

11.6 Claims under this SLA must be made within 20 business days of restoration of the fault. Customer should submit claims in writing to their Account Executive.

12. Commencement and Termination of Service

12.1 Service period starts as soon as it is provisioned and Customer is connected to Telarus Public Cloud Connect service.

12.2 Telarus may terminate the Public Cloud Connect service upon any of the following cases:

(a) We reasonably confirmed Customer's attempts to access or modify unauthorized system information, or to interfere with Telarus environment normal operations.
(b) We reasonably believe there is excessive or unusual use of the service.
(c) We reasonably believe Customer is unlawfully using the service.
(d) We reasonably believe Customer's use of the service infringe any third party's intellectual property rights.

13. Update of Service Terms

13.1 This Service Terms may be modified and updated from time to time based on business requirements. Telarus will provide a 10 business days' notice in advance of the actual implementation of any changes by Customer nominated contact to Customers.

13.2 When we change the Service Terms and notify the Customer, the Customer's continued use of the service signifies the automatic acceptance of the latest version service terms.