Telarus Managed Security

(TMS)

Service Terms

Version 1.0

24th Mar 2016

Table of Contents

1. Introduction

1.1 This section defines the Service Terms of the Telarus Managed Security (TMS) 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

- "**Access Control List (ACL)**" means a list of email and account contact details of Customers which are used to access TMS service and be the unique contact in the change request process. The email address can be the same with Customer Nominated Contact.
- **"Content Category"** indicates the lower-level classification of web page contents under the Content Group.
- **"Content Group"** indicates the classification of web page contents based upon the Web content viewing suitability of three major groups of customers: enterprises, schools, and home/families.
- **"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.
- **"Design Document"** means in the initial provisioning or change management phase of TMS service, the documents which needs mutual agreement between Telarus and Customer regarding TMS service policy settings, testing plans, back out process, etc.
- **"Force majeure"** means an event or circumstance beyond the reasonable control of Telarus.
- **"Minimum Term"** means the minimum period of time calculated in months during which Customer agree to subscribe for the TMS service. It may not be less than 12 months and is mutually agreed between Customer and Telarus in the Service Order.
- **"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.
- **"Service Order"** means a form approved by Telarus, made by the customer for the provision of Services be Telarus.
- **"SSL"**, Secure Socket Layer is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.
- **"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 Product"** means the managed security solution between external public Internet and Telarus managed private network, which is constituting Managed Firewall, Content Intelligence, and Business Reporting.
- **"UAT"**, User Acceptance Testing indicates the process in which actual software users test the software to make sure it can handle required tasks in real-world scenarios, according to specifications.
- **"Unavailability"** means a service resource is failing to perform within a tolerance of 30% of its defined operating parameters.

3. TMS Offerings

3.1 Telarus provides the following tailored TMS product offerings, Customers may select to modify the policies and templates in each of the component:

(a) Telarus Managed Firewall
(b) Content Intelligence
(c) TMS Business Reporting

3.2 There is a default collection of service resource and capabilities provided to customers, which is presented in the table below:

TMS Feature	Metric
Security Zones	3
Service Speed	10Mbps
Authentication	Local
Vulnerability Scanning	6 Monthly – Scan & report
DoS - DDoS Protection	IDS / IPS
WIFI Controller	Disabled
Email - Anti Virus	Enabled – (SMTP, POP3, iMAP, HTTP, HTTPS
Email – Spam Filtering	Enabled – Tag and or Drop

Email – Spam Filtering	0 Domains
Self Service reporting	Enabled
Remote Access - IPSEC	5 Concurrent Users
Remote Access – SSL	10 Concurrent Users
VPN – Point 2 Point	1 Remote Site
Two Factor Authentication	Disabled
Web Filtering Groups	3 Groups
Application Control	0 Applications

3.3 Customers may apply for an additional service resource through placing a Service Order to Telarus. The options for the additional service resource are presented in the table below:

TMS Feature	**Metric**
Security Zones	4, 5 or 6
Service Speed	20, 30, 50, 80, 100 or 200Mbps
Authentication	RADIUS, LDAP & Active Directory
Vulnerability Scanning	Monthly – Scan & Review
DoS - DDoS Protection	Arbour Pravail – Signature based filtering
WIFI Controller	Enabled – 1, 2, 5, 10 or 20 Access Points
Email – Spam Filtering	1, 2, 3, 5 or 10 Domains
Self Service reporting	Enabled
Remote Access - IPSEC	10, 20 or 50 - Concurrent Users
Remote Access – SSL	20, 50, 100 or 200 - Concurrent Users
VPN – Point 2 Point	2, 5, 10 or 20+ Remote Sites
Two Factor Authentication	Enabled (Requires LDAP or AD Authentication)
Web Filtering Groups	5 or 10 Groups
Application Control	5, 10 or 20 Applications

3.4 The availability for Customer's application of additional service resource will be analysed by Telarus on a case-by-case basis.

4. Contract and Payment

4.1 Telarus TMS product has a minimum contract term of 1 months if the TMS product is bound to a Telarus VDC (Virtual Data Centre) product. Otherwise, customers can select a fixed time contract of 12/24/36 months.

4.2 Payment for the TMS product is required to be conducted in advance. The first payment is required at the service commencement date. Customers need to pay for the service monthly.

5. Billing

5.1 Billing is issued monthly.

5.2 Customer adjustments of services are billed monthly in arrears.

5.3 Invoices can be delivered by mail, by fax, or electronically to Customer Nominated Contact, depending on the selection of Customers.

6. Account and Passwords

6.1 Customers will be assigned to a combination of account and initial password details to log in to the TMS service upon their service commencement date.

6.2 Customers can change the password any time and are responsible for keeping their password confidentiality. Telarus will not keep anything regarding to Customer passwords.

6.3 Telarus assumes that any access to Customer account or service using the correct password is authorized by the Customer. Customers are responsible for preventing any unintended access to their account and service. Customers will still be charged for usages of services if their account is used by a third party.

7. Managed Firewall

7.1 TMS firewall will only be responsible for the protection between the public Internet and the managed private network.

7.2 The protection inside the managed private network need 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.

7.3 Customer is solely responsible for complying with license terms of all security products installed on customer self-managed networks and maintain valid licenses.

7.4 Telarus Managed Security (TMS) is supplied as a standard component of Telarus IaaS product. If a Customer is detected to have a security breach within the private network which may lead to adverse impact to other Customers or the whole network, Telarus may suspend the IaaS service of that Customer.

8. Content Intelligence

8.1 TMS Content Intelligence is applied on a best-effort basis. Telarus does not guarantee all contents within the filtered categories will not pass through the TMS service.

8.2 Telarus will be solely responsible for the updates of TMS Content Intelligence. Customers acknowledge that the updates will be automatic and occur via pull mechanism.

8.3 Telarus Antivirus will only scan files up to 10MB in size. By default, files over 10MB in size will be allowed with notification to Customer nominated contact and Customer will be responsible to handle these files using their self-managed antivirus solution.

8.4 By default, Telarus Antispam will tag the spam email in the subject header and forward to Customer's internal mail server. Customer is responsible for the treatment of the tagged spam emails.

8.5 For Telarus Web Content Filtering, Telarus is solely responsible for the management and updates for the 6 Content Groups and more than 80 Content Categories. Telarus will provide 10 business days' notice in advance of the actual implementation of any updates on Content Groups or Categories by Customer nominated contact to Customers.

8.6 Customers acknowledge that Content Groups and Categories will be updated from time to time, and their content filtering policies should be based on the classification of groups and categories.

8.7 Customer may apply to allow specific sites within an otherwise filtered otherwise filtered Content Category. By default, up to 10 specific entries are available for a Customer. Should Customers require more than 10 entries, addition scoping is required and the Change Management Process should be followed.

9. Business Reporting and Data Usage

9.1 The access to TMS Business Reporting is via a secure Internet SSL portal. Access will only be enabled for Customer contacts listed on the Access Control List (ACL) for TMS service.

9.2 Telarus will monitor the TMS Business Reporting data to detect risks and abnormal activities. Telarus will not provide access to Customer data to a third party other than law enforcement agencies.

9.3 If Telarus is required to provide Customer data by law enforcement agencies, we will send a Customer notice to Customer Nominated Contact with a valid state of federal legal request.

9.4 Customer usage of inbound internet data (data downloaded to IaaS environment from Internet) for their IaaS service will be monitored and calculated based on TMS Business Reporting – Traffic Details Report.

9.5 When Customer data usage of all private network services exceeds their applied allocation according to TMS Business Reporting, Telarus will send a notice to Customer nominated contact. Telarus will also send a warning message to Customer nominated contact when Customer data usage reaches 50% and 80% thresholds of their applied allocation. Customer may choose to pay for the excessive usage, or to change to a higher-allocation plan by placing a Service Order to Telarus. If the Customer does not place an order before the end of Calendar month, Telarus will charge the excessive usage by default.

9.6 If the Customer choose to have a higher-allocation data usage plan, the allocation and charges will take effect from the month in which Customer place the Service Order for the changes.

10. Design and Provisioning

10.1 Before the provisioning of TMS service, there should be a design phase in a project-managed, collaborative manner between the Customer and Telarus. It includes but is not limited to the policy and rule settings of the following:

(a) Managed Firewall security policy
(b) Antivirus filtering rules
(c) Default filtering behaviour for files with more than 10MB in size
(d) Default measures for emails which are identified as spams
(e) Content Groups and Category customization: predefined and dynamic rules
(f) Granular customization for specific entries
(g) Business reporting templates
(h) Customer ACL account
(i) Notification contact and mechanism

10.2 Customer may change the policies, rules, or parameters at any time during the design phase. The design phase is concluded by Customer's signed-off version of Design Document, which is a summary of the policies and rules in Term 3.9.1.

10.3 Except for the failure in Customer UAT testing, any changes after the design phase will need to go through the Change Management Process.

10.4 Except for the failure in provisioning, Telarus will not take any responsibility for incorrect agreed policy settings in the design phase.

10.5 Customers acknowledge that any of the additional resource or capability they require in the design phase will incur Telarus professional services and extra charges for the provisioning.

10.6 Before the build and provisioning process, Customer is required to complete the UAT testing summary and provide the impact assessment to Telarus via email. Telarus will not start the build process when these documents are not received.

10.7 After the build process, if the Customer UAT testing fails, Telarus will go back through the design process with Customer until the TMS service can meet Customer requirements and working normally.

10.8 Telarus will not be responsible for any risks or incorrectness in TMS operation if they are due to the faults or negligence in Customer UAT testing.

10.9 TMS service provisioning will take up to 20 business days after Telarus acknowledge Customer's sign-off of Design Document. Extended provisioning time may be required depending on Customer's selection of additional service resource and capabilities.

11. Service Change Management

11.1 Telarus may cancel any service capability or change service charges at any time. The changes will take effect after Customer's current contract period expires.

11.2 There is a standard Change Management Process for the TMS service, any changes that Customer applies for after the previous sign-off of Design Document will need to go through this process. All configuration changes relating to network traffic enforcement, policy or information handling are made by mutual agreement.

11.3 Customer needs to Contact Telarus NOC team via a formal email from Customer contact in the ACL list to start the Change Management Process. Telarus will not process the change request and notify Customer via ACL list contact if the sender of change request email is not included in the ACL list.

11.4 All changes must be signed off by the Customer or authorised delegate prior to implementation. In case of UAT testing failure after change implementation, Telarus will also provide a back out plan to be signed off by Customer.

11.5 Customers acknowledge that there may be service outage for changes of TMS service. Telarus will negotiate the time and date of change implementation with Customer in line with business requirements and acceptable outage windows.

11.6 After the change implementation, if the Customer UAT testing fails, Customer may choose to retry the test plan, or ask Telarus to execute the back out process.

11.7 If Customer chooses to execute the back out process, Telarus will inform Customer via contact in the ACL list once the process is complete. Customer may choose to cancel the changes, or re-start the change design process with Telarus.

11.8 Telarus is solely responsible for preventing any data loss or damage during the period of change implementation.

12. Demarcation

12.1 We don't promise that the TMS service will:

(a) protect against all unauthorised access to your network;
(b) remove all viruses or correctly identify all viruses;
(c) screen or block all spam or correctly identify all spam;
(d) detect and remove all types of attacks or correctly identify all attacks;
(e) block all websites you ask us to block or correctly identify websites that you've asked to be blocked; or
(f) block all network activity you ask us to block or correctly detect and protect against network activity that you deem suspicious.

12.2 Customer will be solely responsible for their connection to the TMS service if they connect via public Internet access or BYO network. Telarus will provide no guarantee of latency or bandwidth.

12.3 Customer will be solely responsible for the correct configuration and implementation of their self-managed security solution for their private network. You are required to deploy a security solution to prevent the risks within the Telarus managed network.

12.4 If we reasonably detect and confirm that the risks from Customer's self-managed network cause adverse effect to other Customers or interfere with normal operation of TMS service, Telarus may suspend the TMS service for the specific Customer and notify via Customer nominated contact requiring Customer for correction within a certain period of time. Telarus reserves the right to terminate Customer TMS service and contract without refund if Customer fails to correct within the timeframe.

12.5 Customer may require an extended correction period by mutual agreement with Telarus.

12.6 Telarus will not be responsible for the service outage or unavailability caused by force majeure of data centres.

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

13. Data Retention

13.1 After service cancellation date, Customer Data relating to the TMS service will be irretrievable and Telarus takes no responsibility for keeping them once a service is cancelled.

13.2 Telarus may keep the meta data relating to TMS 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

14. Service Levels and Rebates

14.1 Telarus Provides a Service Level Target of 99.9% for TMS service.

14.2 The TMS service is a fail secure product. In the unlikely event there is service degradation within managed resources the network communications will be severed in the interests of protecting your business.

14.3 The Service Level Availability (SLA) represents the percentage of time Telarus TMS service is expected to be available during calendar month. It is calculated as: (Service hours – Unavailable hours) / Service Hours * 100%.

14.4 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.

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

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

14.6 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 4 hours	Not Available
More than 4 hours but less than 6 hours	15%
More than 6 hours	30%

14.7 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.

15. Commencement and Termination of Service

15.1 Service period starts as soon as it is provisioned and Customer can access the TMS service. Once Telarus confirms the TMS service is ready, we will notify the Customer by Customer Nominated Contact.

15.2 Telarus may terminate the TMS 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.

15.3 For each Service Order the Minimum Term nominated upon the service order will be upheld. Customer may request to terminate the TMS service at any time.

15.4 When the service termination is requested prior to the elapsed Minimum Term identified upon the Service Order, Customer will be required to pay all remaining monthly reoccurring charges and any incurred once off charges.

15.5 When the service termination is requested after the Minimum Term identified upon the Service Order has elapsed, the service termination date will be 30 calendar days from Telarus' receipt of the request for service termination.

16. Update of Service Terms

16.1 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.

16.2 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.