OUR CUSTOMER TERMS
CLOUD SERVICES – SYMANTEC ENDPOINT PROTECTION

CONTENTS

Click on the section that you are interested in.

OUR CUSTOMER TERMS
CLOUD SERVICES – SYMANTEC ENDPOINT PROTECTION

Certain words are used with the specific meanings set out below or in the General Terms section of Our Customer Terms.

1 ABOUT THE SYMANTEC™ ENDPOINT PROTECTION SECTION

1.1 This is the Symantec Endpoint Protection section of Our Customer Terms. Depending on the nature of the products and services you are receiving under this Cloud Services section, provisions in other parts of the Cloud Services section, as well as in the General Terms of Our Customer Terms at http://www.telstra.com.au/customer-terms/business-government/index.htm, may apply.

1.2 Unless you have entered into a separate agreement with us which excludes them, the General Terms section of Our Customer Terms also applies. See section one of the General Terms of Our Customer Terms at http://www.telstra.com.au/customer-terms/business-government/index.htm for more detail on how the various sections of Our Customer Terms are to be read together.

1.3 See section one of the General Terms of the Cloud Services section for more detail on how the various parts of the Cloud Services section are to be read together.

2 SYMANTEC ENDPOINT PROTECTION APPLICATIONS

What is Symantec Endpoint Protection?

2.1 The Symantec Endpoint Protection application is an anti-virus and anti-malware application which helps:

(a) protect your users computers from detected malware based on known methods; and

(b) block known malicious attacks from the network on the users computer;

(c) block suspected phishing attacks on supported browsers; and

(d) block or allow access from USB storage devices, based on how you configure the application.

Eligibility

2.2 You must:

(a) ensure your computer(s) meets the requirements set out on our Telstra Apps Marketplace Support pages at http://www.telstra.com/marketplacesupport or as otherwise advised by us from time to time;

(b) ensure that your computer(s) and software on your computer(s) are compatible for the Symantec Endpoint Protection application; and

(c) regularly check the default email address that we have allocated to you for messages about your Symantec Endpoint Protection application.

3 APPLICATION FEATURES

3.1 The table below describes each of the applications

Application	Description
Symantec Management Console	Symantec Management Console is a browser based administration console which lets you perform tasks, schedule events, run reports, perform configuration and configure your security applications.
Anti-Virus/Anti-Spyware	Analyses downloaded files and applications to help protect your laptops, desktops and servers from viruses, worms, Trojans, spyware, bots, zero-day threats and root kits.
Intrusion Detection/Prevention	Intrusion Prevention scans your network traffic stream to help detect and prevent threats or methods used to get malicious files onto your network.
Desktop Firewall	Desktop firewall sets up a two-way, rules-based firewall.
Web Security Application	Web security application provides a warning to users regarding suspected dangerous websites.

Your responsibilities

3.2 You must install the Service Software on each users computer.

3.3 You must manage the Service Software, computers, policies, alerts and reports and other configuration options through the Symantec Endpoint Protection management console ("management console").

3.4 You are responsible for any required firewall changes to allow the Symantec Endpoint Protection application to communicate and operate correctly.

Limitations

3.5 We will use reasonable care and skill in providing the Symantec SaaS Endpoint Protection application. However, we do not guarantee that:

(a) all potential viruses and spyware will be detected or removed;

(b) all unauthorised access to your network will be prevented;

(c) our web security application will pick up all dangerous websites; and

(d) only files infected with viruses, spyware, trojans and worms and other malware will be removed.

Software

3.6 Each running instance of the Service Software must be licensed. An "instance" of Service Software is created by executing the Service Software's setup or install procedure or by duplicating an existing instance. You "run an instance" of software by loading it into memory and executing one or more of its instructions. Once running, an instance is considered to be running (whether or not its instructions continue to execute) until it is removed from memory.

3.7 If the Service Software is for use on a hardware device/server that provides endpoints with a common connection point to a local or wide area network (a "**Licensed Terminal Server**"), and such Licensed Terminal Server(s) is/are accessed by endpoints that do not have installed copies of the Service Software ("**Thin Clients**"), then every Thin Client accessing a Licensed Terminal Server is considered an "instance" and must have a license. In the event that the Licensed Terminal Server(s) is/are accessed by endpoints which have authorized copies of the Service Software already installed ("**Thick Clients**"), such access of the Licensed Terminal Server(s) by Thick Clients shall not be considered additional "instances" and you are not required to purchase additional licenses of the Service Software.

Export Controls

3.8 The Service Software for the Symantec Endpoint Protection applications is of United States origin for the purpose of United States export controls. You must comply with all applicable national and international laws that apply to the Service Software including the United States Export Administration Regulations. You must not to directly or indirectly export, import or transmit the Service Software contrary to the laws or regulations of any governmental entity that has jurisdiction over such export, import, transmission or use.

Your Data

3.9 All logs and reports created by the Symantec Endpoint Protection application are stored on, viewable and downloadable from the management console for a period of 12 months from creation. The logs are automatically deleted at the end of the 12 month period.

Audit

3.10 We (or a third party acting on our behalf) may periodically audit you on reasonable notice to ensure that you are complying with your obligations regarding the Symantec Endpoint Protection application (including the Service Software).

User numbers

3.11 You must select a minimum of 5 user licences for each Symantec Endpoint Protection application

3.12 If you apply to add additional users, the Initial Term for each additional user will expire at the same time as the Initial Term for your initial application. If adding the additional users moves your subscription into a new pricing tier, all users under your subscription will be charged on the basis of that new tier from the date you increased the users.

3.13 If you wish to remove a number of users from your subscription (e.g. decrease the number of users under your subscription) you can decrease the number of users from your subscription in the Telstra Apps Marketplace. If your plan or individual user licences is cancelled before your minimum term has ended, you'll need to pay us an Early Termination Charge (ETC) for each user licence cancelled. The ETC is calculated as 65% of the monthly charge multiplied by the number of user licences cancelled multiplied by the number of remaining months in your plan term, plus the set up charge (if there is one).

4 CHARGES

4.1 We will charge you a monthly charge for your Symantec Endpoint Protection applications as set out in the Telstra Apps Marketplace.

5 TERM AND TERMINATION

5.1 You may take up the Symantec Endpoint Protection applications for an Initial Term of twelve (12), twenty four (24) or third six (36) months (each an **"Initial Term"**).

5.2 If your Symantec Endpoint Protection application is cancelled (other than for our material breach) during the Initial Term, we may charge you an early termination charge calculated as 65% of the monthly charges for the subscription multiplied by the number of remaining months in the Initial Term at the date of termination, plus any set up charges (if there is one).

6 SERVICE LEVELS

What are our service levels?

6.1 Unless a service level exclusion applies, we aim to meet the service levels for your application set out in the table below. Service levels do not apply during any trial period for the application. You acknowledge that our service levels are targets only and we will not be responsible for failing to meet them.

Application	availability target
Symantec Endpoint Protection	99.9%

Service level exclusions

6.2 We will not be liable for failure to meet a Service Level which:

(a) is an intermittent period for less than 10 minutes;

(b) is caused by you or as a result of your negligence or breach of an obligation including any breach by you or your users of obligations under T-Suite Our Customer Terms;

(c) is caused by you or your users failing to follow our reasonable directions;

(d) arises from you providing us with full and accurate information about the incidents that you report to us;

(e) is attributable to an event not reasonably within our control or our sub-contractor's control;

(f) results from any problems or unavailability of internet connectivity or your internal network;

(g) occurs during Scheduled Downtime;

(h) without limiting any of the above, is due to any of the following faults:

  (i) faults caused by hardware, software or systems used by you (such as due to incompatibility), unless such hardware, system, software is provided by us as part of the application;

  (ii) faults caused by you or any person accessing your application using your password or access key or by your invitation;

  (iii) faults caused by your negligence or the negligence of any person accessing your application using your password or access key or by your invitation;

  (iv) faults due to wilful damage to your application by you or any person accessing your application using your password or access key or by your invitation;

  (v) faults with your equipment that have not been caused by us; or

(i) is a result of downtime required by Telstra to implement an emergency or planned outage to perform urgent or maintenance work. We aim to provide you with as much notice (through the Telstra Apps Marketplace) as possible before an emergency outage.