CONTENTS

Click on the section that you are interested in.

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.CLOUD™ SECTION

1.1 This is the Symantec.cloud 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.CLOUD APPLICATIONS

What is Symantec.cloud?

2.1 We provide seven Symantec.cloud packages that you can select from, described in the table below.

		Features						
		Email anti-virus and anti-spam	Email data protection	Email image control	Web anti-spyware and anti-virus	Web URL filtering	Web content filtering	Smart Connect.cloud**
Package	**Symantec.cloud Email Protect**	•						
	Symantec.cloud Email Safeguard	•	•	•				
	Symantec.cloud Web Safeguard**				•	•	•	Option at additional cost
	Symantec.cloud Email and Web Safeguard**	•	•	•	•	•	•	Option at additional cost

	Features						
	Email anti-virus and anti-spam	Email data protection	Email image control	Web anti-spyware and anti-virus	Web URL filtering	Web content filtering	Smart Connect.cloud**
Symantec Email Protect.cloud*	•						
Symantec Email Control.cloud*		•	•				
Symantec Email Protect and Control.cloud*	•	•	•				
Symantec Web Protect.cloud*				•			Option at additional cost
Symantec Web Control.cloud*					•	•	Option at additional cost
Symantec Web Protect and Control.cloud*				•	•	•	Option at additional cost
Symantec Email & Web Protect & Control.cloud*	•	•	•	•	•	•	Option at additional cost

* These packages are no longer available to new customers on and from 29 April 2014.
** These packages are no longer available to new customers on and from 16 November 2018.
Existing customers can continue to use the applications and change user numbers, as permitted below.

Eligibility

2.2 Apart from the Smart Connect.cloud application, you must select a minimum of 5 end user licences for each Symantec.cloud application.

2.3 The Smart Connect.cloud application is only available with a package containing the Web Protect.cloud, Web Control.cloud or Symantec.cloud Web Safeguard application.

2.4 Your email system or other relevant system must be permanently connected to the Internet with a fixed IP address.

2.5 We cannot provide the Symantec.cloud application to you if your email system or other relevant system is connected to the Internet through dial-up or ISDN lines or where the IP address of your email system or other relevant system is dynamically allocated.

User numbers

2.6 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.

2.7 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 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). You may reduce the number of Smart Connect.cloud users without incurring an early termination charge.

3 APPLICATION FEATURES

3.1 The applications available with the various Symantec.cloud packages are described in the table below.

Application	Description
Email anti-virus and anti-spam	Email anti-virus checks nominated emails being sent to an email address for most known viruses, trojans and worms and filters emails where these are picked up. Email anti-spam identifies senders of unsolicited email from reaching a nominated email address. You can configure your application to take certain actions with the suspected spam.
Email data protection	Email content control filters certain email based on the rules that you set.
Email image control	Email image control detects pornographic images contained in image files attached to emails. You can configure your application to take certain actions with suspected pornographic images.
Web anti-spyware and anti-virus	Web anti-spyware and anti-virus enables certain webpages to be electronically routed through the application to assist with protecting your computers from known spyware and viruses. Access to the web anti spyware and anti virus application is restricted via "Scanning IP" which are the IP address(es) from which your web

Application	Description
	traffic originates. The Scanning IPs are also used to identify the customer and dynamically select customer-specific settings. The web anti spyware and anti virus application will scan as much of the web page and its attachments as possible. It may not be possible to scan certain web pages, content or attachments (for example, password protected or encrypted content).
Web URL and content filtering	Web URL and content filtering are designed to filter out certain URLs or access to certain web pages based on an access restriction policy that you determine. Access to the web URL filtering application is restricted via "Scanning IP" which are the IP address(es) from which your web traffic originates. The Scanning IPs are also used to identify you and dynamically select your specific settings. You are responsible for configuring the web URL filtering application to create access restriction policies (based both on categories and types of content) and deploy these at specific times to specific users or groups.
Smart Connect.cloud	Application that extends web protection and policy enforcement to users roaming outside your corporate network. You may only use this application if you also have Symantec Web Protect.cloud and/or Symantec Web Control.cloud application(s). The application may not be used in any country identified as a 'no service' country by Symantec. The current 'no service' countries are listed here: http://images.messagelabs.com/EmailResources/ServiceAdminGuides/WebRoamingAgent/SmartConnect_NoServiceCountries.pdf When your users connect to the internet, any HTTP and FTP-over-HTTP requests (including attachments, macros or executables) are redirected by the application through the Web Protect.cloud and/or Web Control.cloud application(s) as applicable. The policy rules configured in your Web Protect.cloud and/or Web Control.cloud application(s) will also be applied when the user uses the Smart Connect.cloud application. You are responsible for configuring the application to direct traffic to the Web Protect.cloud and/or Web Control.cloud application(s). You must install the application software (a PAC file) onto each Users computer, so that the browser is pointed to the application when the user's browser is accessed. You may not transfer the application software to any third party who is not one of your employees except that you may allow your sub-contractors to use the application provided you notify them of and they agree to comply with the terms and conditions for Smart Connect.cloud.

Limitations

3.2 We will try to scan all of the email or its attachments, macros or executables that are directed through the email anti virus application for known viruses.

We may not be able to scan certain content, for example password protected or encrypted content.

3.3 We will use reasonable care and skill in providing the Symantec.cloud application. However, we do not guarantee that:

(a) all spam emails will be detected or that any email identified as spam is actually spam;

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

(c) all content configured to be detected or pornographic images will be detected, or that any image detected as a pornographic image is actually pornographic in nature;

(d) unauthorised access to your network will be prevented; and

(e) all websites that have specified to be blocked by you, will be blocked.

3.4 A Symantec.cloud application may:

(a) prevent some emails not infected with viruses from reaching you;

(b) cause a delay in the delivery of emails to you; and

(c) block certain websites that you have not specified to be blocked.

3.5 If you identify one of the above limitations in a Symantec.cloud application, you should notify us immediately and to the extent possible, we will endeavour to rectify the issue at no additional charge.

3.6 We and our external suppliers are not responsible for any liability to any person resulting from:

(a) information passing through the Symantec.cloud application from you; and

(b) any delivery or non-delivery of an email, web page, image or other content,

(c) where that liability is not directly or indirectly attributable to us or our external supplier's breach of Our Customer Terms or negligent act or omission.

3.7 You acknowledge that in certain countries you may have to obtain the consent of each individual person to use the Symantec.cloud application.

3.8 You are responsible for checking any local laws applicable to your use of the Symantec.cloud application prior to obtaining the application from us.

3.9 We and our external suppliers do not accept any civil or criminal liability that may be incurred by you as a result of the operation of the Symantec.cloud application or your use of the application.

Export Controls

3.10 The Service Software for the Symantec.cloud application 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 directly or indirectly export, import or transmit the service software contrary to any laws or regulations concerning such export, import, transmission or use.

Audit

3.11 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.cloud application (including the Service Software).

Additional cancellation or suspension rights

3.12 We may immediately cancel or suspend some or all of your Symantec.cloud applications if:

(a) we become aware that your email systems allow unknown or unauthorised third parties to send and/or receive emails from your email systems;

(b) we believe that your continued use of the Symantec.cloud application would compromise the security of this application; or

(c) you fail to comply with the export controls set out above.

3.13 If we cancel your Symantec.cloud application you must return to us or destroy (at our choice) any documentation and other materials relating to our or our external supplier's business that you may have under your possession or control.

4 CHARGES

4.1 The charges for your Symantec.cloud applications will depend on the packages that you select.

4.2 We will charge you a monthly charge for each package that you have (as set out in the Telstra Apps Marketplace).

5 TERM AND EARLY TERMINATION CHARGE

5.1 Apart from the Smart Connect.cloud application, you must take up the Symantec.cloud applications for an initial term of twelve (12), twenty four (24) or thirty six (36) months (**"Initial Term"**). You may take up the Smart Connect.cloud application on a casual (month to month) basis.

5.2 If you terminate any of your Symantec.cloud applications apart from Smart Connect.cloud, (other than for our material breach) or if you signed up or renewed your Symantec.cloud application on and from 28 February 2013,

we terminate or cancel your Symantec.cloud application for your 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 any).

6 SYMANTEC.CLOUD SAFEGUARD SERVICE LEVELS

6.1 The capitalised terms below have the following meaning:

"**Credit Request**" means the notification you submit to us via submitting a service ticket through Telstra Apps Marketplace Support and ensure credit request is included in the ticket'.

"**Designated Tower Cluster**" means two (2) or more Towers designated to provide Email Security Applications to you.

"**Email Security Applications**" are the Symantec.cloud Email Protect and Symantec.cloud Email Safeguard applications.

"**Email Virus False Positive**" means a legitimate email incorrectly identified as containing a Virus.

"**Known Virus**" means a Virus for which at the time of receipt of the content by Symantec:

(a) a signature has already been made publicly available for a minimum of one (1) hour for configuration by anti-Virus technologies used by Symantec; or

(b) is included in the "Wild List" held at http://www.wildlist.org and identified as being "In the wild" by a minimum of 2 Wild List participants.

"**Service Availability**" for:

(a) Email Security Applications means the ability to establish a SMTP session on port 25 of the Designated Tower Cluster, as measured by Symantec Tracker where the Designated Tower Cluster is able to:

(i) receive your inbound email on behalf of your domain on a 24x7 basis; and

(ii) accept your outbound email from your correctly configured SMTP host on behalf of your domain(s) on a 24x7 basis.

(b) Web Applications means the availability of the Web Applications to accept Customer's outbound web requests and shall only apply if your host, gateway devices or proxy(s) are correctly configured on a 24x7 basis

"**Spam**" means unsolicited commercial email.

"**Spam False Negative**" means a Spam email that is not identified as Spam by the Email AntiSpam.cloud application.

"**Spam False Positive**" means an email incorrectly identified as Spam by the Email AntiSpam.cloud application.

"**Spam Recommended Settings**" means the recommended configuration guidelines for the Email AntiSpam.cloud application as provided to you during the provisioning process or as published in the Symantec online help resource.

"**Symantec Tracker**" means a Symantec tool by which Service Availability and latency are measured for the Email Security Applications.

"**Tower**" means a cluster of load balanced Email servers.

"**Validation List**" means a list of specific email addresses to receive the Symantec.cloud Safeguard applications.

"**Unknown Virus**" means a Virus for which at the time of receipt of the content by Symantec:

(a) a signature has not already been made publicly available for a minimum of one (1) hour for configuration by anti-Virus technologies used by Symantec; or

(b) was not included in the "Wild List" held at http://www.wildlist.org and identified as being "In the wild" by a minimum of 2 Wild List participants.

"**Virus**" means a piece of program code, including a self-replicating element, usually disguised as something else, which is designed so that it may infect other computer systems

"**Web Applications**" means the Symantec.cloud Web Safeguard application.

6.2 If you believe you are entitled to a remedy in connection with a service level in this clause 6, you must:

(a) promptly raise a service ticket through Telstra Apps Marketplace Support, providing details of the incident;

(b) submit a Credit Request to us within five (5) business days of raising the service ticket and no later than ten (10) business days of the end of the calendar month in which the suspected breach of the service level occurred. The Credit Request must reference the service ticket reference we provide to you.

6.3 All Credit Requests will be subject to verification by us.

6.4 The service levels in this clause 6 do not apply:

(a) during periods of planned or emergency maintenance, periods of non-availability due to force majeure, your acts or omissions or third party acts or omissions;

(b) during any period of suspension or where you are in breach of the the terms (including where you have overdue payments) for your Symantec.cloud Safeguard application;

(c) if you have not configured the Symantec.cloud Safeguard application correctly;

(d) to any emails that have not passed through the Email Security Applications (including if you have not taken appropriate steps to ensure that you will only accept inbound email from the Symantec infrastructure); or

(e) in respect of any inbound or outbound emails that were initially sent to Symantec containing more than 500 recipients per SMTP session.

6.5 The service levels for the Email Security Applications do not apply to the Email Continuity.cloud application and the:

(a) 100% service availability service level;

(b) 100% email delivery service level; and

(c) Email latency – 60 seconds service level,

will be suspended during any period in which the Email Continuity.cloud application is in an activated state.

6.6 The remedies set out in this clause 6 will be your sole and exclusive remedy for a breach of the service levels for your Symantec.cloud Safeguard application(s).

6.7 Our maximum accumulative liability to you for a breach of the service levels for your Symantec.cloud Safeguard application(s) in any calendar month shall be no more than one hundred percent (100%) of the monthly charge of the affected Symantec.cloud Safeguard application(s).

6.8 Where the affected Symantec.cloud Safeguard application is part of a non-severable bundle:

(a) for the purpose of calculating service credits, the monthly charge for the affected Symantec.cloud Safeguard application will be calculated as the total monthly charge for the non-severable bundle divided by the number of separate Symantec.cloud Safeguard applications included in the bundle; and

(b) if you terminate the affected Symantec.cloud Safeguard application in accordance with this clause 6, the revised charge for the non-severable bundle will be calculated as the original total monthly charge for the non-severable bundle, divided by the original number

of separate Symantec.cloud Safeguard applications included in the bundle, and multiplied by the number of remaining Symantec.cloud Safeguard applications in that bundle.

100% Service Availability

6.9 This Service Availability service level will only operate if you use the Email Security Applications or Web Applications.

6.10 If in any calendar month Service Availability is below one hundred percent (100%), you may submit a Credit Request and may receive a Service Credit for the following percentage credit:

Percentage service availability per calendar month	Percentage credit of monthly charge
< 100% but >= 99%	25%
< 99% but >= 98.0%	50%
< 98.0%	100% and termination of affected Email Security Application at your discretion

100% Email Delivery

6.11 This email delivery service level will only apply if you use one or more of the Email Security Applications.

6.12 Symantec will deliver 100% of all email sent to or from you, subject to the following:

(a) the email must have been received by your Designated Tower Cluster; and

(b) the email must not contain a Virus, Spam or other content which has caused it to be intercepted by the Email Security Applications.

6.13 Subject to provisions above above, in the event Symantec fails to deliver an email to or from you, you may chose to terminate the Email Security Applications upon thirty (30) calendar days prior written notice.

Email Latency – 60 Seconds

6.14 This email latency service level will only operate if you use one or more Email Security Applications but does not apply to the Policy Based Encryption application.

6.15 If in any calendar month the average roundtrip time (as measured by the Symantec Tracker) for emails sent every 5 minutes to and from every Email Security Applications Tower within your Designated Tower Cluster exceeds

the delays stated in the table below, you may submit a Credit Request and may receive a Service Credit in accordance with the table below:

Average roundtrip time of 100% of measurements (in minutes and seconds)	Percentage credit of monthly charge
> 1 min but <= 1min 30 secs	25%
> 1min 30secs but <= 2 mins	50%
> 2 mins but <= 2mins 30 secs	75%
> 2 mins 30 secs	100%

6.16 This email latency service level do not apply:

(a) if you have not supplied a Validation List and you suffers a denial of service attack;

(b) during periods of delay caused by a mail loop from/to your systems; or

(c) if your primary email server is unable to accept email on the initial attempted delivery.

Web Latency – 0.1 Seconds

6.17 This web latency service level only applies if you use one or more Web Applications and only applies to objects of 1MB or less.

6.18 If the average scanning time of web content, measured from when Symantec receives the content to the point of Symantec's attempted transmission of the content, calculated over the course of a calendar month is less than 100%, you may submit a Credit Request and may receive a Service Credit in accordance with the table below:

Average percentage of web content scanning within 100 milliseconds	Percentage credit of monthly charge
< 100% but >= 99%	25%
< 99% but >= 98%	50%
< 98% but >= 97%	75%
< 97%	100% and termination of affected Web Application at your discretion.

Spam – False Positives 0.0003%

6.19 This Spam False Positive service level only applies if you use the Email AntiSpam.Cloud application and implement the Spam Recommended Settings and only applies to inbound emails.

6.20 Where the average Spam False Positive capture rate rises above 0.0003% of your email traffic in any calendar month you may be submit a Credit Request and may receive a Service Credit in accordance with the table below:

Percentage Spam False Positive capture rate during the calendar month	Percentage credit of monthly charge
>0.0003 but <= 0.003	25%
> 0.003 but <= 0.03	50%
>0.03 but <= 0.3	75%
>0.3	100%

6.21 The following emails will not constitute Spam False Positive emails for the purposes of this service level:

(a) emails which do not constitute legitimate business email;

(b) emails containing more than 20 recipients;

(c) emails where the sender of the email is on your blocked senders list, including without limitation those defined by your individual user if you have enabled user-level settings;

(d) emails which are sent from a compromised machine;

(e) emails which are sent from a machine which is on a third party block-list;

(f) emails which have at least 80% of the same content; or

(g) emails intercepted by outbound spam scanning.

99% Spam Capture Rate

6.22 This Spam capture service level only applies if you use the Email AntiSpam.Cloud application and implement the Spam Recommended Settings and only applies to inbound emails.

6.23 The provisions of this service level correspond to the number of Spam False Negatives measured in a calendar month.

6.24 Where the Spam capture rate in any calendar month is not met, you may submit a Credit Request and may receive a Service Credit in accordance with the table below:

Percentage Spam Capture rate during the calendar month	Percentage credit of monthly charge
>98% - <= 99%	25%
> 97% - <= 98%	50%
> 96% - <= 97%	75%
< 96%	100%

6.25 This Spam capture service level will not apply where the email was not sent to a legitimate address.

6.26 A lower Spam capture rate of 95% applies to emails containing more than 50% double byte character sets. Where the Spam capture rate falls below 95%, you may be entitled to a 25% Service Credit of the monthly charge. Where the Spam capture rate falls below 90%, you may be entitled to a Service Credit equal to 100% of the Monthly Charge.

Spam Credit Requests

6.27 In order to be eligible for a credit under the Spam False Positive and Spam capature service levels, you must report and send suspected False Positive or False Negative Emails to the Support Helpdesk within five (5) calendar days of receipt of the email. We will investigate and confirm whether or not the email is a Spam False Positive or Spam False Negative and will record the finding. You must also submit a Credit Request in accordance with clause 6.2 if you are seeking a Service Credit.

Email Virus Protection – 100% Known and Unknown

6.28 This email Virus protection service level only applies if you use the Email Protect or Safeguard application and you have configured the application correctly.

6.29 If your systems are infected by one or more Known or Unknown Viruses, by an email that passed through the Email AntiVirus.cloud application, in any calendar month, you may be entitled to a Service Credit in the amount stated below.

6.30 You must notify us as soon as you become aware that a Virus has been passed to you through the Email AntiVirus.cloud application. You must also submit a Credit Request, and if validated, will receive a Service Credit equal to the lower of 100% of the monthly charge for the affected application(s) or ten thousand Australian dollars (AUD$10,000). The remedy set out in this clause does not apply to cases of deliberate self-infection.

6.31 Your systems are deemed to be infected if a Virus contained in an email received through the Email AntiVirus.cloud application has been activated within your systems either automatically or with manual intervention.

6.32 In the event that Symantec detects, but does not stop a Virus-infected email, we (or Symantec) will promptly notify your designated support contact(s), providing sufficient information to enable you to identify and delete the Virus-infected email.

6.33 The remedy set out above does not apply if:

(a) such notification results in a prevention of infection; or

(b) you fail to promptly act upon the notification.

6.34 The Email Protect or Safeguard applications will scan as much of the email and its attachments as possible. It may not be possible to scan attachments with content which is under the direct control of the sender (for example, password protected and/or encrypted attachments). Such Email and/or attachments are excluded from the service level and the remedy set out above does not apply.

6.35 This email Virus protection service level does not apply to Viruses intentionally released by you.

6.36 This email Virus protection service level does not apply to other types of malware, including, but not limited to; Trojans; Phishing; Spyware; Adware; or URL links to websites hosting malicious content.

Email Virus False Positives 0.0001%

6.37 This Email Virus False Positive service level only applies if you use the email Virus protection application.

6.38 Where the Email Virus False Positive capture rate rises above 0.0001% of the email traffic in any calendar month you may submit a Credit Request and may receive a Service Credit in accordance with the table below:

Percentage Spam Capture rate during the calendar month	Percentage credit of monthly charge
>0.0001 but <= 0.001	25%
> 0.001 but <= 0.01	50%
>0.01 but <= 0.1	75%
>0.1	100%

Web Virus Protection – 100% Known

6.39 This web Virus protection service level only applies if you use the Web Safeguard Service.

6.40 Your systems are deemed to be infected if a Known Virus contained in a web transaction received through the Web Safeguard application has been activated within your systems either automatically or with manual intervention.

6.41 If your systems are infected by one or more Known Viruses, by a URL that passed through the Web Safeguard application, in any calendar month you may be entitled to a Service Credit in the amount stated below.

6.42 You must raise a service ticket via the Support Helpdesk as soon as you become aware of an infection and provide details of the URL from which the item was downloaded. You must also submit a Credit Request in accordance with clause 6.2 if you are seeking a Service Credit. If validated, you will receive a Service Credit up to a maximum amount equal to the lower of the monthly charge for the affected application or ten thousand Australian dollars (AUD$10,000). The remedy set out in this clause does not apply where you have deliberately self-infected or downloaded known malicious code.

6.43 Your systems are deemed to be infected if a Known Virus contained in a web transaction received through the Web Safeguard application has been activated within your systems either automatically or with manual intervention.

6.44 In the event that Symantec detects but does not stop a Known Virus as part of a URL which passed through the Symantec Web Safeguard Service, we (or Symantec) will promptly notify you, providing sufficient information to enable you to identify and delete the item.

6.45 The remedy set out above does not apply if:

(a) such notification results in a prevention of infection; or

(b) you fail to promptly act upon the notification.

6.46 The Web Safeguard Service will scan as much of the Web item downloaded as possible. It may not be possible to scan items that are encapsulated or tunneled for communication purposes via the supported Web Protocols (HTTP, and FTP over HTTP), conveyed over HTTPS, compressed or modified from their original form for distribution, product license protection, download or update, or content which is under the direct control of the sender (for example, password protected and/or encrypted items). Such items and/or attachments are excluded from the service level and the remedy above does not apply.