



## SECURITY SAAS – SYMANTEC.CLOUD + SERVICE ATTACHMENT

### Part I: Rates and Charges.

### Part II: Service Description and Requirements.

### Part III: Service Terms and Conditions.

### Part IV: Definitions

**Part I: Rates and Charges.** Customer will pay the monthly recurring charge (“MRC”) and nonrecurring charges (“NRC”) shown in the Customer’s Contract, and at the following URL: [www.verizonenterprise.com/external/service\\_guide/reg/applicable\\_charges\\_toc.htm](http://www.verizonenterprise.com/external/service_guide/reg/applicable_charges_toc.htm) based upon the Symantec.cloud services ordered (each, individually a “Symantec Service” and collectively, “Symantec Services”). Customer will be invoiced the MRC upon the Service Activation Date. As used herein “Verizon” includes Symantec Corporation as the provider of Symantec Services. Verizon reserves the right to audit the number of end users Customer has on Symantec Services, and in the event that the number of end users of Symantec Services exceeds the number of end user subscriptions ordered by Customer, Verizon reserves the right to charge Customer for the difference, or, if the difference is significant, to take other appropriate steps, including suspending and/or terminating Symantec Services.

1. **Service Commitment.** The Service Commitment for each Symantec Service is shown in the applicable Contract. The minimum Service Commitment is 12 months. Customer may order additional subscriptions at any time and each order will have its own Service Commitment, and each order will be billed at the then-current rates. Unless Verizon or Customer provides notice of termination of all or part of an order 45 days prior to the expiration of a Service Commitment, each order will automatically renew for a minimum period of 12 months (and will be considered a new order). Verizon reserves the right to change the MRC to be effective at the beginning of a new Service Commitment with 60 days’ notice prior to the expiration of the then current Service Commitment. If: (a) Customer terminates a Symantec Service or any subscription before the end of the relevant Service Commitment for reasons other than Cause; or (b) Verizon terminates Symantec Services for Cause, then Customer will pay an amount equal to the relevant MRC for the terminated subscriptions remaining during relevant Service Commitment or Service Commitments.

### Part II: Service Description and Requirements.

1. **Service Description.** Symantec Services provides network-based services to manage, secure, protect, control, encrypt and archive electronic communications. Symantec Services include the infrastructure, customer portal used for administration, service management, reporting, and helpdesk support. Information on these features as well as a service description and terms and conditions for each Symantec Service can be found at <http://www.symanteccloud.com/documents.aspx> (the “Service Description”). All capitalized terms used but not defined herein have the meanings given to such terms in the Agreement or in the Service Description. The current Symantec Services are:
  - 1.1 **Email Security.cloud.** Email Security.cloud is inbound and outbound messaging security, with antimalware, anti-Spam, content filtering, and Email encryption services from a global cloud platform.
  - 1.2 **Volume Mail.** Volume Mail allows end users to send and receive bulk Email not categorized or filtered as Spam.
  - 1.3 **Boundary Encryption.cloud.** Boundary Encryption.cloud service provides confidentiality of Email communications by setting up private Email networks with encryption for both sender and recipient.
  - 1.4 **Policy Based Encryption.cloud.** Policy Based Encryption.cloud is a hosted service that helps safeguard the security and privacy of data that end users exchange with customers and business partners via Email.
  - 1.5 **Web Security.cloud.** Web Security.cloud helps protect an organization from Web-borne threats and enables the control, monitoring and enforcement of acceptable use policies
  - 1.6 **Enterprise Vault.cloud.** Enterprise Vault.cloud is a cloud-based archiving service to store and manage information in an online repository, with end user access and search functionality.
  - 1.7 **Endpoint Protection.cloud.** Endpoint Protection.cloud Small Business Edition 2013 offers protection for computer systems against viruses and malware.
  - 1.8 **Web Portal.** The web portal for Symantec Services (the “Portal”) provides web-based information, resources, support, and configuration of Symantec Services with a dashboard view of service statistics, summary and detailed reporting features. Portal also provides functionality for managing user and domain data. Portal features include:
    - **Email Services Dashboard.** A real time visual snapshot of Email security statistics.

## SECURITY SAAS – SYMANTEC.CLOUD + SERVICE ATTACHMENT

- Summary Reports. A PDF overview of Email security statistics with graphs, tables, and key statistics relating to overall Email volume and service performance.
  - Detailed Reports. A CSV file containing detailed Email statistics for each individual service.
  - Service administration facilitates the configuration of services.
  - Email anti-virus, anti-Spam, image control, and content control configuration and reports.
  - Web security services configuration and reports.
2. **Symantec Services Acceptance.**
- 2.1 **Acceptance Process.** Verizon will notify Customer of the date when each Symantec Service ordered by Customer is ready for use. Thereafter, Customer has ten days (“Verification Period”) to verify that the Symantec Service complies the applicable features, function, performance and/or other attributes of, and requirements for, Symantec Services in the Services Descriptions (the “Specifications”). Customer may reject all or any portion of Symantec Services within the Verification Period. Upon any rejection, Customer, in its sole discretion, may elect to: (a) give Verizon twenty days from receipt of notice of rejection to correct Errors or other nonconformity at no charge and to redeliver corrected Symantec Services; or (b) terminate the Symantec Services. Rejection of Symantec Services may be made via fax, Email, mail, or courier service.
3. **Symantec Services Terms.**
- 3.1 Customer is responsible for implementing the configuration options for Symantec Services through the Portal.
- 3.2 Customer may request customization of eligible portions of the End User portal up to a maximum of two times per 12 month period.
- 3.3 Verizon reserves the right to withhold provision or suspend all or part of the Symantec Services if it feels that Customer’s violation of the provisions below poses an immediate threat to the integrity of the Symantec Services. Customer shall not allow its Email systems to:
- 2.3.1 act as an Open Relay; or
  - 2.3.2 send or receive bulk Email or send Spam; or
  - 2.3.3 compromise the security of Symantec Services (without limitation, to hacking attempts, denial of service attacks, mail bombs, or other malicious activities either directed at or originating from Customer’s domains).
- 2.4 Symantec Services may be provided from any hardware installation forming part of the Symantec Services anywhere in the world and the provision of Symantec Services may, at any time, be transferred from one installation to another. No installation, or part thereof, is dedicated to the sole use of Customer.

**Part III: Service Terms and Conditions.** In addition to the terms and conditions found in the Service Description, the following terms and conditions apply.

1. **Intellectual Property Rights.** Each party agrees that except as provided below, it acquires no right, title or interest in or to the other party’s information, data base rights, data, tools, processes or methods, or any copyrights, trademarks, service marks, trade secrets, patents or any other intellectual or intangible property or property rights of the other party by virtue of the provision of Symantec Services. Customer retains all right title and interest in and to the underlying factual data gathered through the provision of Symantec Services. Verizon owns all right title and interest in and to trade secrets, confidential information or other proprietary rights in any creative or proprietary ideas, information or other material used by Verizon or presented to Customer (each, a “Technical Element”), including, but not limited to: data, software, modules, components, designs, utilities, databases, subsets, objects, program listings, tools, models, methodologies, programs, systems, analysis frameworks, leading practices, report formats, manner of data expression and specifications. Verizon grants Customer a nonexclusive, royalty-free license to use each Technical Element integrated into Symantec Services solely for Customer’s internal business purposes. Customer may disclose a Technical Element integrated into a deliverable to a third party as long as such third party is subject to a written nondisclosure agreement, requiring such third party to maintain the confidentiality of such Technical Element and use such Technical Element only for the benefit of Customer. Notwithstanding anything contained in this Service Attachment to the contrary, Customer is prohibited from creating derivative works of all or any portion of a Technical Element.
- 1.1 Customer will not: (i) copy or otherwise reproduce, whether in whole or in part, Symantec Services to which Customer has been granted access or use; (b) modify or create any derivative work of Symantec Services; (c) sell, rent, loan, license, sublicense, distribute, assign or otherwise transfer Symantec Services; (d) cause or permit the disassembly, decompilation or reverse engineering of any software components of Symantec Services or otherwise attempt to gain access to the source code of such software components; or (e) cause or

## SECURITY SAAS – SYMANTEC.CLOUD + SERVICE ATTACHMENT

permit any third party to do any of the foregoing. Such restrictions shall survive the expiration or termination of this Service Attachment or the Agreement.

2. **Scanning.** Customer understands that website or Email scanning, including, without limitation, the scanning of applications, and the technology associated with it (collectively “Scanning”), has risks, including, but not limited to, the loss, disruption, or performance degradation of Customer’s or a third party’s business processes, or data (the “Scanning Risks”). Customer acknowledges that it understands and accepts the Scanning Risks associated with Symantec Services and authorizes Verizon to perform the Symantec Service when ordered. Verizon shall take reasonable steps to mitigate these Scanning Risks (e.g. by using limited requests per second so as to run in the background); however, Customer understands that these Scanning Risks cannot be eliminated. Customer agrees to indemnify, defend and hold harmless Verizon and its affiliates, officers, agents, successors or assigns (each, a “Verizon Indemnified Party”) from and against any and all loss, damages, liabilities, costs and expenses (including legal expenses and the expenses of other professionals) incurred by Verizon, resulting directly or indirectly from any third-party claim attributable to or arising out of Verizon’s use of “Scanning Technology” (each, a “Scanning Claim”), including, without limitation, the use by Verizon of “Scanning Technology” to analyze assets that are not controlled directly by Customer (e.g., servers hosted by third parties). The obligation of Customer to indemnify, defend and hold a Verizon Indemnified Party harmless in connection with a Scanning Claim will not apply to the extent that the Scanning Claim is based on Verizon’s gross negligence or willful misconduct.
3. **Warranty and Limitation of Liability.** Except as otherwise stated herein, the parties agree that Verizon, its independent contractors and suppliers are providing Symantec Services on a “WHERE IS, AS IS” basis and make no warranties, express or implied, statutory or otherwise, and specifically disclaim all implied warranties (including those of availability, reliability, usefulness, merchantability, non-infringement, fitness for a particular purpose and those arising out of course of performance, dealing, usage or trade). The Customer accepts that no anti-virus, anti-Spam, image control, or content control service can guarantee 100% detection rate and Verizon will not be liable in respect of any failure of a Symantec Service to detect web content, Spam or pornographic images or for wrongly identifying as any Email or web page content suspected as being a web page to be restricted or as being Email containing Spam or pornographic which proves subsequently not to be so. Verizon does not warrant that Symantec Services are uninterrupted or error-free or that any web applications scanned, software, or any other materials accessed through Symantec Services are free from infringing materials, viruses, malicious codes and other harmful components. For services provided to Customer from third parties and third party products, Customer receives only the warranties offered by such third party either directly or to the extent Verizon may pass through such warranties to Customer.
4. **Nature of Service.** Symantec Services does not provide service, maintenance or repair to or for any real or personal property.
5. **Service Level Agreement.** The Service Level Agreement (“SLA”) for Symantec Services, which is made a part of the Agreement, sets forth Customer’s sole remedies for any claim in connection with Symantec Services and is located in the Service Description.
6. **Customer Data.** Customer (and not Verizon) is responsible for taking any steps that may be required by law or otherwise to inform end users and others sending and receiving Email from or to the domains receiving Symantec Services that such Email is subject to scanning for Viruses, Spam, pornographic images and/or textual content as described in this service attachment, and as a result the Email’s traffic data, header information and/or content may be accessed for that limited purpose. As a part of that limited purpose, Verizon (including its suppliers used in providing this service) may use any Virus-, Spam-, pornography-related or text violated content to (i) maintain and improve the performance and integrity of Symantec Services, (ii) observe, study and test the functioning of Symantec Services; (iii) comply with regulatory, legislative or contractual requirements (including cooperating with law enforcement authorities); and (iv) make available to licensors information passing through Symantec Services for the purposes of enhancing Symantec Services and protecting against Viruses, Spam, pornography and tagged, blocked or logged textual content. Customer acknowledges that the United States and other countries regulate the treatment of Email and other information and will comply with all applicable data protection, privacy and similar laws in its use of Symantec Services and that Verizon is not liable for any use of Symantec Services by Customer in a manner that is inconsistent with legal requirements or use of Symantec Services by Customer beyond the above limited purpose.
  - 6.1 In certain jurisdictions the use of components of Symantec Services may be restricted by law and/or it may be necessary to obtain the consent of or provide adequate notice to individual end-users or third parties, including but not limited to employees of the Customer or persons impacted by Symantec Services, and/or where required, inform, consult or agree with employee representatives, and/or to file a declaration with the appropriate data protection authority and/or to take other steps prior to and in connection with the monitoring or filtering of electronic communications traffic using Symantec Services or parts thereof. Verizon makes no representation

## SECURITY SAAS – SYMANTEC.CLOUD + SERVICE ATTACHMENT

as to where or if such requirements or any other requirements apply in the jurisdiction where Customer deploys Symantec Services or any other jurisdiction where such deployment has an effect. It is Customer's responsibility to obtain its own legal advice as it deems necessary and to comply with any applicable data protection, privacy, law, regulation, codes of practice or other requirement prior to deploying and otherwise in connection with the ongoing operation of Symantec Services. Customer undertakes that it will investigate and comply with all such laws and regulations, codes and requirements.

- 6.2 Customer acknowledges and agrees that the configuration of Symantec Services components and its implementation is entirely within the control of the Customer. In particular, Symantec Services with image control and content control are intended to be used solely to enable the Customer to enforce an existing, effectively implemented acceptable computer use policy (or its equivalent), to the extent permitted by applicable law and regulations. Customer undertakes to ensure at all times that the configuration of such image control and content control is in compliance with such policy and applicable laws and regulations in the affected jurisdictions. Verizon accepts no liability that may be incurred by the Customer as a result of the operation of Symantec Services. The Customer recognizes that, for instance, the definition of what does and does not constitute a pornographic image may be subjective or subject to legal and regulatory requirements and this should be taken into account during Customer's configuration of the image control option.
- 6.3 Without limiting the generality of the foregoing, Customer shall ensure that in its use of the Anti-Spam, Image Control and Content Control Symantec Services options, it complies with the following usage restrictions:
- 6.3.1 Customer must not use the anti-Spam, image control, or content control Symantec Services options, if its corporate mail server is located within Germany (DE), Austria (AT), Switzerland (CH), France (FR) or Argentina (AR);
- 6.3.2 Any domain, top level domain or subdomain that references DE, AT, CH, FR or AR will be excluded from the anti-Spam, image control, or content control Symantec Services options (i.e. top level domains or subdomains with either top level domain extension of .de, .at, .ch, .fr, .ar or respective subdomain(s)); and
- 6.3.3 Customer must not use the anti-Spam, image control, or content control Symantec Services options to scan in- or outbound Email traffic to/from such employees or other end users who are based within DE, AT, CH, FR or AR and/or spend more than half of their working time within these countries ("Restricted Recipients"); in particular, if the company's domains include any Email addresses of Restricted Recipients, Customer must ensure that Restricted Recipients are excluded from the anti-Spam, image control, or content control Symantec Services options by setting up appropriate sub-domains for those Restricted Recipients and excluding such sub-domains from scanning for such options, or by comparable technical means.
- 6.4 Customer shall indemnify Verizon and Verizon's associates, officers, directors, employees, agents and partners in respect of any and all claims, regulatory actions, losses, damages, costs and expenses suffered or incurred directly or indirectly by Verizon and Verizon's associates, officers, directors, employees, agents and partners from or arising out of Customer's failure to ensure the necessary compliance with applicable laws, regulations and other requirements, including the above usage restrictions.
- 6.5 Customer acknowledges that, Verizon does not have access to, control or influence over the content of any Emails processed by Symantec Services and, to the extent that any Emails consist of or contain personal data as such term is defined in the EU Directive 95/46/EC, Verizon is not a data controller of such personal data and will only process the same on the instructions of the Customer, who shall be considered as the data controller of such personal data. Customer undertakes to comply with any data protection, applicable regulation, and submit all required notification or authorization request to the relevant data protection authorities.
7. **Privacy User.** Customer has the option to designate individual employees as "Privacy Users" and allow these Privacy Users to control certain service features as may be required by applicable privacy legislation. Privacy User designation is carried out by the Customer via the Portal. The Customer is responsible for managing the Privacy Users list from within the Portal interface. Any user Email addresses that are placed on the Privacy Users list will have additional flexibility and/or restrictions depending on the configuration at the time of provisioning. Privacy User lists are managed on a per domain basis.
- 7.1 All Privacy Users are opted out of the anti-Spam, image control or content control Symantec Service options during the initial deployment. Privacy Users will be provisioned with the flexibility to opt into or out of each such service from within the Portal. Each Privacy User will receive an individual account creation mail with instructions for use of the Portal.

## SECURITY SAAS – SYMANTEC.CLOUD + SERVICE ATTACHMENT

7.2 Customer administrators can only access a Privacy User's account by using paired administration and the view of the account will be restricted, limiting functionality to review and release only.

8. **Export Compliance.** The parties acknowledge that the export restrictions and service locational limitations set forth in the Guide and in the Service Description shall apply. In addition to these restrictions and limitations, Customer shall not, and shall not permit any third party to, sell, resell, export, re-export, transfer, divert, distribute, dispose of, disclose or otherwise deal with the Symantec Services technology, directly or indirectly, to any of the following countries: Afghanistan, Angola, Armenia, Azerbaijan, Bosnia and Herzegovina, Burma, Burundi, China, Cuba, Democratic Republic of Congo, Eritrea, Ethiopia, Iran, Iraq, North Korea, Liberia, Libya, Nigeria, Rwanda, Sierra Leone, Somalia, Sudan, Syria, Tanzania, Uganda and Zimbabwe.

**Part IV: Definitions.** In addition to the definitions identified in the Master Terms, the following administrative charge definitions apply to Symantec Services:  
[www.verizonenterprise.com/external/service\\_guide/reg/definitions\\_toc\\_2017DEC01.htm](http://www.verizonenterprise.com/external/service_guide/reg/definitions_toc_2017DEC01.htm)