Validation & ID Protection (VIP) Service

Service Description

July 2018

Service Overview

This Service Description describes Symantec's *Validation & ID Protection* ("VIP" or "Service"), which includes its enabling components. All capitalized terms in this Description have the meaning ascribed to them in the Agreement (defined below) or in the Definitions section.

This Service Description, with any attachments included by reference, is part of and incorporated into Customer's manually or digitally-signed agreement with Symantec, which governs the use of the Service, or if no such signed agreement exists, the Symantec Online Services Terms and Conditions (hereinafter referred to as the "Agreement").

Table of Contents

1. TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

Service Overview

VIP is a multi-factor authentication platform. The Service provides online service providers and enterprises with increased security of their applications in the form of multi-factor authentication and protection for their End Users against account takeover. The Service also enables End Users to utilize a single Authenticator across all VIP-enabled service providers and enterprises.

This Service Description outlines the primary elements of the Service and describes the roles and responsibilities of all the entities necessary to provide strong authentication to End Users.

Service Features and Components

The Service leverages a shared validation infrastructure operated by Symantec that enables Customer to deploy and accept multi-factor authentication without bearing the entire burden of managing and operating their own self-standing authentication infrastructure. By allowing End Users to leverage a single Authenticator to secure their transactions at multiple enterprises, Symantec VIP helps make it simpler for End Users to adopt stronger authentication.

Subject to Exhibit B (Service Level Agreement), the Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis and is monitored for service capacity and network resource utilization. The Service is regularly monitored for service level compliance and adjustments are made as needed.

Key features and components:

- VIP Authenticators
- VIP Web Services Application Programming Interfaces (APIs) and Integrations
- VIP Manager
- VIP Self-Service Portal
- Audit Trails and Audit Retention
- Service Enabling Software

VIP Authenticators

An "**Authenticator**" is something End User possesses and controls (typically a cryptographic module) that is used to authenticate End User's identity. The Service provides and supports several different types of VIP Authenticators: hardware- and software-based, as well as Out-Of-Band (OOB) Authenticators.

- **VIP OTP Tokens, Cards, and VIP Access software Authenticators –** These Authenticators are single-factor one-time password (OTP) Authenticators that generate OTPs. These are hardware Authenticators and software-based OTP generators installed on devices such as mobile phones and personal computers. These VIP Authenticators consist of a unique VIP Credential ID and an embedded secret, shared with the Service, that is used as the seed for generation of OTPs and does not require activation through a second factor. The "VIP Credential ID" is an alphanumeric string that can vary in length from 12 to 16 characters, which identifies both the VIP Authenticator manufacturer as well as the VIP Authenticator itself. This VIP Credential ID can be bound to a "User ID," which can be any string that uniquely identifies an End User within Customer. The OTP is displayed on the device and manually input by End User for transmission to the Service for verification, thereby proving possession and control of the device. An OTP device may, for example, display 6 characters at a time. These VIP Authenticators are anonymous and provide a second authentication factor as something End User has when it is associated to a local user identity of Customer.

  The hardware-based Authenticators purchased from Symantec come with a three (3)-year warranty as described in the Warranty Information Supplement available in the Repository at https://www.symantec.com/about/legal/repository (or its successor webpage), which is listed under "*Validation & ID Protection (VIP) Service.*"

- **Multi-Factor One Time Password (OTP) Authenticator** - These Authenticators are multi-factor one-time password

Authenticators that generate OTPs. A multi-factor OTP Authenticator generates OTPs for use in authentication after activation through an additional authentication factor. Only hardware-based Authenticators are available for this category. The second factor of authentication is achieved through some kind of integrated entry pad. The OTP is displayed on the Authenticator and manually input by End User for transmission to the Service for verification, thereby proving possession and control of the Authenticator. This VIP Authenticator is anonymous and provides a second authentication factor as something End User has when it is associated with a local user identity of Customer. The multi-factor OTP Authenticators something you have, and it will be activated by something you know.

- **VIP Security Key –** These are single-factor cryptographic Authenticators that operate by signing a challenge nonce presented through a direct computer interface (e.g., a USB port). The Authenticator uses embedded symmetric or asymmetric cryptographic keys, and does not require activation through a second factor of authentication. These Authenticators have a unique VIP Credential ID, and authentication is accomplished by proving possession of the Authenticator via the Universal 2nd Factor (U2F) authentication protocol. The VIP Security Key is a multi-modal Authenticator and can also generate an OTP. This VIP Authenticator is anonymous, and provides a second authentication factor as something End User has when it is associated with a local user identity of Customer.

- **VIP Trusted Device -** This Authenticator is a single-factor cryptographic software. This Authenticator consists of a cryptographic key stored on disk and associated with a unique VIP Credential ID. It utilizes a browser plug-in to manage cryptographic keys generated and stored in a proprietary keystore on End User's device. Authentication is accomplished by proving possession of the device. The Authenticator's output is provided by direct connection to the user endpoint, facilitated by the browser plug-in, and consists of a signed message. This is used as a second authentication factor when it is associated with a local End User identity at Customer.

- **VIP Push –** This is an Out-of-Band (OOB) authentication mechanism that allows the Service to send a push notification to a uniquely addressable VIP Access software Authenticator on a device in possession of End User (where VIP Push is available). The Service then waits for the establishment of an authenticated protected channel and verifies the Authenticator's identifying key and a digital signature over the contents of the message sent to the device. This signature along with End User's approval or denial of the push notification provides a second authentication factor as something End User has when it is associated with a local user identity of Customer.

- **VIP SMS OTP –** This is an Out-of-Band Authentication mechanism that allows the Service to send an OTP via a text message to an End User's SMS capable mobile device. The SMS text message contains a numeric OTP, securely generated by the Service, along with a message specified by Customer. The OTP is then manually input by End User for transmission to the Service for verification, thereby proving possession and control of the SMS device. This is used as a second authentication factor when it is associated to a local End User identity at Customer.

  SMS OOB Authentication is an additional service that may be purchased for an additional fee as a corollary to the VIP Authentication Service.

- **VIP Voice OTP –** This is an Out-of-Band Authentication mechanism that allows the Service to send an OTP via a voice call to an End User's voice capable device. The voice call contains a numeric OTP, securely generated by the Service, along with a message specified by Customer. The OTP is then manually input by End User for transmission to the Service for verification, thereby proving possession and control of the device. This is used as a second authentication factor when it is associated with a local End User identity at Customer.

  Voice OOB Authentication is an additional service that may be purchased for an additional fee as a corollary to the VIP Authentication Service.

VIP Web Service APIs and Integrations

- **VIP Web Service APIs** – The Web Service APIs fall under five categories. Each handles different operations necessary for Customer to authenticate their End Users with a strong second factor:

Management APIs – These APIs allow Customer to create and/or associate a new Authenticator with their VIP account. They also allow Customer to add, update, or delete a user or groups of users with the Service. They allow Customer to assign, update, or remove an Authenticator to an End User, and send an OTP to an End User. These also let Customer manage the state of Authenticators.

Query APIs - These APIs allow Customer to obtain information about an Authenticators as well as End Users, such as when a user was created in VIP, when an Authenticator was last bound to the user, when the user was last authenticated, etc.

Authentication APIs - These APIs allow Customer to authenticate an Authenticator or an End User based on verification of proof of possession of their Authenticator.

Policy APIs – These APIs allow Customer to set policies that control the behavior of the Service as it relates to End Users and Authenticators

Reporting APIs - Significant events are recorded by Symantec on a transaction-by-transaction basis. Symantec maintains audit records independently in multiple media depending upon the sensitivity of the event. Audit trails are created for all management, query, and authentication transactions. These APIs allow the Relying Party to obtain these audit records.

- **VIP Login** – VIP Login provides strong authentication using industry standard federation protocols. Integrating using VIP Login with the Service provides a flexible, standard means for securely authenticating End Users to common web applications that support federated identities.
- **VIP Intelligent Authentication** – VIP Intelligent Authentication builds a risk profile for login events, and generates a risk score by analyzing End User's device profile, behavioral patterns, location, network connection and other factors. Depending on the risk associated with a particular login event, Customer can "step up" authentication using out-of-band or two-factor authentication techniques supported within the enterprise or through the Service.

VIP Manager

VIP Manager is a web-based portal, hosted by Symantec, for the configuration and management of the Service. Customer is given access to this portal for the purposes of configuring Service parameters, viewing reports, and managing End Users and Authenticator Lifecycle Functions. In addition, VIP Manager keeps audit logs that record functions executed by individual Administrators. Access to VIP Manager is controlled by validating either: (i) the Administrator's email address, password, and VIP Authenticator, or (ii) the Administrator's enterprise username and password through a single sign-on functionality enabled by either the VIP Enterprise Gateway or an enterprise-hosted SAML-compliant federation server, in addition to validating the Administrator's VIP Authenticator.

VIP Self-Service Portal

VIP Self-Service Portal is a web based portal, hosted by Symantec, for End Users' VIP Authenticator Lifecycle Functions-related services. Customer can grant direct access to this VIP Self-Service Portal to their End Users. Access to the VIP Self-Service Portal is controlled by validating an End User's enterprise username and password through a single sign-on functionality enabled by either the VIP Enterprise Gateway or an enterprise-hosted SAML-compliant federation server.

Audit Trails and Audit Data Retention

Significant events are recorded by Symantec on a transaction-by-transaction basis. Symantec maintains audit records independently in redundant media and locations depending upon the sensitivity of the event. Audit trails are created for all authentication, query, and management transactions, and End User self-service and Administrator operations.

All audit information is maintained for 12 months from the time of event for online retrieval, and indefinitely for retrieval upon request.

Service Enabling Software

This Service includes the following enabling software, which should be used only in connection with Customer's use of the Service during the Subscription Term. Use of the enabling software is subject to the license agreement accompanying such software ("Software License Agreement"). If no Software License Agreement accompanies the software, it is governed by the terms and conditions located at http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf. In the event of conflict, the terms of this Service Description prevail over any such Software License Agreement. Customer must remove enabling software upon expiration or termination of the Service.

Any maintenance/support purchased for the Service shall also apply to Customer's use of the Service Enabling Software.

Customer's use of the following software is optional.

- **VIP Enterprise Gateway** – This is a 'self-hosted' software component deployed by Customer. It may be provided for the integration of enterprise applications and directories. VIP Enterprise Gateway enables multi-factor authentication by utilizing a first and layering multiple second-factors of authentication. The first factor, can be a password associated with each End User, which is stored in the enterprise directory. The second-factor can be one of the many Authenticators as supported by the Service. The second factor validation is performed by the Service. For each validation request sent to the VIP Enterprise Gateway, the first-factor validation is performed locally at the enterprise directory. VIP Enterprise Gateway then completes the second factor authentication against the Service. VIP Enterprise Gateway also records audit logs that record authentication events that are processed through it.

  The Service also includes documentation and custom plug-ins (where necessary) that layer multi-factor authentication on top of many popular enterprise applications that require End User access.

  The respective documentation and custom plug-ins (where necessary) are distributed on-line. The website is updated on a regular basis with new integrations.

  Software License Agreement - Available in the Repository at https://www.symantec.com/about/legal/repository (or its successor webpage), and listed under "*Validation & ID Protection (VIP) Service*."

- **VIP Access Manager** – This is a 'self-hosted' software component deployed by Customer. It offers single sign-on with strong authentication, access control, and user management in a unified solution. Additionally, this solution allows Customer to extend internal security policies to public and private cloud services in support of compliance and auditing requirements. It is a virtual software appliance, including the Single Sign-On ("SSO") portal and the administrator portal, that is responsible for enforcing access policies for the Service. The administrator portal permits certain designated and authorized users to add Connectors, polices, and user stores (or authentication sources). The SSO gateway is a virtual software appliance that Customer deploys on a virtual machine. It enables End Users to authenticate against single or multiple user stores. It supports several user stores as defined in the installation guide, including, but not limited to Microsoft Active Directory, LDAP, IWA, ADFS, and third-party identity providers which support identity federation. Administrators can control which cloud applications an End User may access by defining policies, based on End User's identity and session context and enforce strong authentication. Administrators can also create Connectors to various service providers from the application catalog.

  This component also includes a generic Connector template to allow integration with an application not currently published in the application catalog. VIP Access Manager records important security events to create audit trails that can be transmitted to a log management and SIEM solution. Customer can archive the logs according to its requirements and internal policies.

  Software License Agreement - Available in the Repository at https://www.symantec.com/about/legal/repository (or its successor webpage), and listed under "*Validation & ID Protection (VIP) Service*."

- **VIP Access Software Authenticators (for Mobile and Desktop)** – VIP Access is a software Authenticator that is made available to Customer's End Users. This software is an application that is compatible with various mobile and personal

computer operating systems. VIP Access offers End User the capability to authenticate to the Service using an OTP or a VIP Push, where available.

Software License Agreement – Available in the Repository at https://www.symantec.com/about/legal/repository (or its successor webpage), and listed under "*Validation & ID Protection (VIP) Service.*"

- **VIP Mobile Software Development Kit (SDK)** – The VIP Mobile Software Development Kit, sometimes referred to as the Credential Development Kit (CDK), is a software development kit for iOS and Android mobile operating systems. The SDK is typically useful for mobile application developers who prefer to add VIP second factor authentication, transaction signing, and risk based authentication capabilities to their custom mobile application.

  Software License Agreement - Available in the Repository at https://www.symantec.com/about/legal/repository (or its successor webpage), and listed under "*Validation & ID Protection (VIP) Service.*"

Service Level Agreement

Symantec provides the availability service level agreement ("SLA") for the Service as specified in Exhibit-B.

2. CUSTOMER RESPONSIBILITIES

Symantec can only perform the Service if Customer provides required information or performs required actions, otherwise Symantec's performance of the Service may be delayed, impaired or prevented, and/or eligibility for Service Level Agreement benefits may be voided as noted below.

- Setup Enablement: Customer must provide information required for Symantec to begin providing the Service.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist Symantec in delivery of the Service, upon reasonable request by Symantec.
- Renewal Credentials: If applicable, Customer must apply renewal credential(s) provided in the applicable Order Confirmation within its account administration, to continue to receive the Service, or to maintain account information and Customer data which is available during the Subscription Term.
- Customer Configurations vs. Default Settings: Customer must configure the features of the Service through the VIP Manager, VIP Enterprise Gateway and VIP Access Manager portals, as applicable, or default settings will apply. In some cases, default settings do not exist and no Service will be provided until Customer chooses a setting. Configuration and use of the Service are entirely in Customer's control, therefore, Symantec is not liable for Customer's use of the Service, nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.
- Installation of Service Enabling Software may be required for enabling certain features of the Service.
- Customer must comply with all applicable laws with respect to use of the Service.
- Customer is responsible for its data, and Symantec does not endorse, and has no control over, what End Users submit through the Service. Customer assumes full responsibility to back-up and/or otherwise protect all data against loss, damage, or destruction. Customer acknowledges that it has been advised to back up and/or otherwise protect all data against loss, damage or destruction.
- Customer is responsible for its account information, password, or other login credentials. Customer agrees to use reasonable means to protect the credentials, and will notify Symantec immediately of any known unauthorized use of Customer account.
- Customer is responsible to obtain all necessary End-User and VIP-Authenticator information and securely transmit requests to Symantec to validate VIP-Authenticator information and coordinate the activation of VIP Authenticators and their association to End Users. For Authenticators where Symantec does not explicitly enforce End User to agree to a license agreement, Customer shall require End User to agree to terms and conditions of VIP-Authenticator usage in a form substantially similar to the form provided by Symantec - the "VIP End User Agreement," found at

http://www.symantec.com/content/en/us/about/media/repository/vip-end-user-agreement.pdf, or in the Repository at https://www.symantec.com/about/legal/repository (or its successor webpage), which is listed under "*Validation & ID Protection (VIP) Service.*"

- Customer is responsible to promptly disable or deactivate any VIP Authenticator:
  - upon fraudulent or suspected fraudulent use;
  - upon notification, that the VIP Authenticator has been lost or stolen; or
  - upon request from its End User.

- Customer is responsible for informing Symantec:
  - of fraudulent or suspected fraudulent use of a VIP Authenticator; or
  - upon notification from End User that their VIP Authenticator has been lost or stolen.

Customer hereby grants Symantec the right to display Customer's logo on Symantec's website(s) in one of the forms shown in Customer's trademark usage guidelines.

Acceptable Use Policy

- Customer is responsible for complying with the Symantec Online Services Acceptable Use Policy.

Customer Service-Specific Warranties

- Customer warrants that all information it provides related to usage for calculating the applicable Meter and/or applicable Fees is accurate and complete.

3. SYMANTEC RESPONSIBILITIES

Symantec is responsible for establishing and maintaining the secure operation of the Service and may take any action that, in its sole discretion, it deems necessary to protect the integrity of the Service. This includes the right to shut down any Customer or to revoke a VIP Authenticator if misuse of either the Service by Customer or the VIP Authenticator is detected or suspected.

Symantec shall use commercially reasonable efforts to secure the systems maintaining VIP software and data files from unauthorized access. Symantec undergoes a periodic AICPA Service Organizations Control (SOC) audit of its infrastructure and supporting services. The most recent SOC audit report is available to Customer upon request.

Symantec is responsible for accrediting different devices for use as VIP Authenticators on the Service and accrediting Symantec VIP partners and resellers.

Symantec shall perform all User and Authenticator Lifecycle Functions and authentication operations on behalf of Customer.

4. ENTITLEMENT AND SUBSCRIPTION INFORMATION

Customer may use the Service only in accordance with the use meter or model under which Customer has obtained use of the Service: (i) as indicated in the applicable Order Confirmation; and (ii) as defined in this Service Description or the Agreement.

Charge Metrics

The Service is available under one of the following Meters as specified in the Order Confirmation:

- Per **User**
- Per **Authenticator**

- Per **Transaction**

Customer grants Symantec the right to limit the number of Authenticators associated with each User. In addition, a "User" or "Authenticator", and associated usage may be determined by Symantec at its sole discretion.

Changes to Subscription

If Customer has received Customer's Subscription directly from Symantec, communication regarding permitted changes of Customer's Subscription must be sent to Symantec through a sales representative or by contacting Symantec Customer Support, unless otherwise noted in Customer's agreement with Symantec. Any notice given according to this procedure will be deemed to have been given when received. If Customer has received Customer's Subscription through a Symantec reseller, please contact the reseller.

Changes to Subscription Meter Amounts

Customer may increase Subscription Meter amount at any time, by submitting an order for additional Services. If current use of the Service exceeds the Meter amount shown on applicable Order Confirmation(s), then Customer must promptly submit a new order for the additional use, which will be invoiced at the then-current rates, or as mutually agreed upon by Customer and Symantec, through the current Subscription Term, and the aggregate Meter amount will be the basis for any renewal of the Subscription. Symantec reserves the right to invoice Customer for any additional use, at the then-current rates, if a corresponding order is not promptly received. Each additional order will be subject to the then-current version of the Agreement.

5. ASSISTANCE AND TECHNICAL SUPPORT

Customer Assistance

Symantec will provide the following assistance as part of the Service, during regional business hours:

- Receive and process orders for implementation of the Service
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions

Technical Support

If Customer is entitled to receive technical support ("Support") from Symantec, the Support as specified in Exhibit-C is included with the Service. If Customer is entitled to receive Support from a Symantec reseller, please refer to Customer's agreement with that reseller for details regarding such Support, and the Support described in Exhibit-C will not apply to Customer.

6. ADDITIONAL TERMS

- The Service may be accessed and used globally, subject to applicable export compliance limitations and technical limitations in accordance with the then-current Symantec standards.
- Any templates supplied by Symantec are for use solely as a guide to enable Customer to create its own customized policies and other templates.
- Customer shall enforce the terms of the VIP End User Agreement against End Users and shall notify Symantec of any known breach of such terms. Customer will defend and indemnify Symantec against all claims and damages to Symantec caused by the failure to include the required contractual terms in each VIP End User Agreement.
- Symantec reserves the right to modify and update the features and functionality of the Service, with the objective of providing equal or enhanced Service (as long as Symantec does not materially reduce the core functionality of the Service). Customer acknowledges and agrees that Symantec reserves the right to update this Service Description at any time during the

Subscription Term to accurately reflect the Service being provided, and the updated Service Description will become effective upon posting.

- If Symantec determines that Customer's aggregate activity on the Service imposes an unreasonable load on bandwidth, infrastructure, or otherwise, Symantec may impose controls to keep the usage below excessive levels. For Inline Service, defined as the query and validation of existing VIP Authenticators and Users, the expected average usage per week is 20 transactions per User or Authenticator and the expected peak usage is 10 transactions per second for Customer. Upon receiving notification (e.g., email) of excessive (vs. expected) usage, Customer agrees to remediate their usage within ten (10) days, or to work with Symantec or its reseller to enter into a separate fee agreement for the remainder of the Subscription Term. If the parties are not able to establish a resolution within ten (10) days after the initial notification, then Symantec may institute controls on the Service or terminate the Service and the Agreement, without liability. In addition, if Symantec determines that the excessive usage may present a risk to the Service, Symantec may implement technical and business measures to bring usage into compliance.

- The Service does not include Customer's configurations, policies and procedures implemented and set by Customer that are available through the Service. Customer acknowledges and agrees that they are solely responsible for selecting their configurations and assuring that the selection conforms to policies and procedures and complies with all applicable laws and regulations in jurisdictions in which Customer is accessing the Service.

- Customer shall advise End Users that they may incur additional charges from their wireless carriers, and shall be solely responsible for such charges when sending and/or receiving any SMS text messages or voice calls, including the SMS text messages and voice calls issued as part of this Service. Symantec shall not be responsible to reimburse Customer or End Users for such charges including, but not limited to, inter-connection, access, termination, pager, wireless, landline or any phone charges in the provision of this Service.

- Customer shall not use the Service to transmit: (i) junk mail, spam, or unsolicited material to persons or entities that have not agreed to receive such material or to whom Customer does not otherwise have a legal right to send such material; (ii) material or data that is illegal, harassing, coercive, defamatory, libelous, abusive, threatening, obscene, harmful to minors, excessive in quantity, or the transmission of which could diminish or harm the reputation of Symantec or any of the carriers involved in the provision of the Service, including but not limited to material that is related to alcoholic beverages, tobacco, guns or weapons, illegal drugs, pornography, crime, violence, death, or any other questionable subject matter.
- When validating a VIP Authenticator within VIP, Symantec determines that the VIP Authenticator is valid and active, and that the OTP value generated from the VIP Authenticator or response to VIP Push is associated with the VIP Credential ID. Symantec makes no representations about VIP Authenticators not supplied by Symantec, and shall not be held liable for damages relating to the use of any VIP Authenticator outside its control.
- **No Service Carry-over.** Any units of the Service which are not consumed during the annual period for which such units were purchased may not be carried over to a subsequent annual period whether or not during the same Subscription Period.

- **Termination Due to End of Service Availability.** The Service (or a portion) may be terminated upon ninety (90) days prior written notice by Symantec, in the event that the Service (or a portion) are affected by Symantec's cessation of, or designation of 'end of life' of, such Service (or a portion).

7. DEFINITIONS

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement or this Services Description, have the meaning given below:

"**Administrator**" means a Customer User with authorization to manage the Service on behalf of Customer. Administrators may have the ability to manage all or part of a Service as designated by Customer.

"**Authenticator Lifecycle Functions**" means the primary management functions related to the lifecycle of any VIP Authenticator, including, activation/deactivation, locking/unlocking, disabling/enabling and synchronization.

"**Connector(s)**" means a hosted application created by Symantec or Customer which allows an Administrator to manage configuration and access to enterprise applications that are available to End Users in the SSO portal.

"Credit Request" means the notification which Customer must submit to Symantec through their sales representative or by contacting Symantec Customer Support.

"**Customer**" means the entity that purchased the Service, including any agents and/or contractors it authorizes to install and use the Service on its behalf.

"**End User**" or "**User**" means Customer's employees, contractors and external users who are authorized by Customer to use the Services on behalf of Customer.

"**Emergency Maintenance**" means unscheduled maintenance periods which during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure or any maintenance for which Symantec could not have reasonably prepared for the need for such maintenance, and failure to perform the maintenance would adversely impact Customer.

"Major Release for Service Enabling Software" means a new release of a VIP Service enabling software component that incorporates the last Minor Release (if one has occurred) and may include additional enhancements to the software. Major Releases may include architectural changes, major feature changes, new platform support, and new operating system support. Major releases may deprecate or remove functionality. Unless otherwise defined via a specific communication, Major Releases are designated by the number to the left of the decimal point such as 1.0, 2.0, 3.0, etc.

"Minor Release for Service Enabling Software" means a new release of a VIP Service enabling software component that incorporates all previous feature updates and fixes since the prior Major Release. A Minor Release is tied to the preceding Major Release and may contain new features, new platform support and new operating system support. Unless otherwise defined via a specific communication, Minor Releases are designated by numbers to the right of the decimal point such as 1.1, 1.2, 1.3, etc.

"Monthly Charge" means the monthly charge for the affected Service(s) as defined in the Agreement.

"**Planned Maintenance**" means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure.

"**Repository**" means the collection of documents located at www.symantec.com (or its successor website) maintained for the purpose of publishing them.

"**Service Credit**" means the amount of money that will be credited to Customer's next invoice after submission of a Credit Request and validation by Symantec that a credit is due to Customer.

"**Subscription Instrument**" means one or more of the following applicable documents which further defines Customer's rights and obligation related to the Service: a Symantec certificate or a similar document issued by Symantec, or a written agreement between Customer and Symantec, that accompanies, precedes or follows the Service.

"Symantec Online Service Terms and Conditions" means the terms and conditions located at or accessed through the Repository at https://www.symantec.com/about/legal/repository (or its successor webpage).

"**Transaction**" means an authentication event as measured by the Service.

EXHIBIT-A

DATA PRIVACY NOTICE

Symantec VIP does not require any End User personally identifiable information (PII) to provide authentication. Symantec does not obtain any End User information associated with any VIP Authenticator unless explicitly provided by Customer. With respect to each VIP Authenticator, Symantec only maintains the shared secret and its unique VIP Credential ID.

A VIP Authenticator can be validated using only its VIP Credential ID or can be associated with a User ID. User ID is a string created by Customer, with the option to use a non-meaningful identifier. Customer may associate other identifying data with User ID for management purposes, such as an email address, but this is not required for authentication. VIP does not need to be aware of the identity of End User at Customer.

Notwithstanding the forgoing, if VIP Intelligent Authentication is activated, Symantec will collect and process the following information about End User and End User's machine:

- Operating system
- IP address
- Browser type
- Network
- Geographic location, which may include city, state or country
- Existing Symantec endpoint software stored on the machine

To collect such information Symantec utilizes a persistent tag in End User's browsers, HTML cookies, various parameters that are made available by the browser and IP address of End User's device. The information is processed for the purpose of determining the User's typical pattern of behavior. During the authentication process, the stored pattern is compared with the actual behavior in order to assess anomalies in a particular log-in event. The information is stored on Symantec's servers in the United States.

All End User data that is collected is encrypted in motion and at rest within the Symantec infrastructure and services. For more information about Symantec privacy practices, see **Product Privacy Notices** and **Transparency Notices** located in the *Privacy Portal*.

EXHIBIT-B

SERVICE LEVEL AGREEMENT

The following service levels are applicable to the Service during the Subscription Term.

1. Availability of the Service.

a. Availability. Availability of the Service is distinguished between Inline Service, Non-Inline Service and Out-Of-Band Delivery Services. Inline Service is defined as the query and validation of existing VIP Authenticators and Users. Non-inline Service is any service that provides management and reporting applicable to VIP. VIP Authenticator and User provisioning, VIP Reporting, VIP Manager, and VIP Self-Service portal with multi-page UI are Non-inline Services. Out-Of-Band delivery services is any service which Symantec provides to deliver one-time passwords or other forms of actionable notifications to End User. SMS text messages, Voice calls and Push notifications are examples of Out-Of-Band delivery services. Inline Service will be generally available 99.95% of the time. Non-inline Service will be available 99.5% of the time. Out-Of-Band Delivery Service will be available 99.5% of the time. Availability is calculated per calendar month as follows:

$$\frac{Total - NonExcused\ Outages}{Total - Excused\ Outages} \times 100 \geq Availability\ Target$$

- Total means the number of minutes for the calendar month
- NonExcused means unplanned downtime.
- Service unavailability will not be assessed due to: (i) a failure of Customer to correctly configure the service in accordance with applicable service documentation or adherence to the Agreement; (ii) the unavailability of a specific web page or a third party cloud application(s) or service provider; (iii) individual data center outage; or (iv) unavailability of one or more specific features, functions, or equipment hosting locations within the service, while other key features remain available.
- Excused Outages include:
    - Planned downtime. With respect to planned downtime, Symantec shall provide Customer with as much notice as practical under the circumstances and strives for a minimum of 48 hours or more of advance notice. Symantec shall make commercially reasonable efforts to schedule planned downtime in off peak hours (local datacenter time).
    - Emergency maintenance. Customer acknowledges that Symantec may, in certain situations, need to perform emergency maintenance (unplanned downtime) on less than 24 hours advance notice.
    - Any unavailability caused by circumstances beyond Symantec's reasonable control, including, without limitation, acts of God, acts of government, flood, fires, earthquakes, civil unrest, acts of terror, strikes or other labor problems (excluding those involving Symantec employees), failures or delays involving hardware, software, network intrusions or denial of service attacks not within Symantec's possession or reasonable control.

For any partial calendar month during which Customer subscribes to the Service, general availability will be calculated based on the entire calendar month, not just the portion for which Customer subscribed.

b. Third Party Factors. Customer acknowledges that, in provisioning the Services contemplated herein, Symantec depends on the facilities, networks, connectivity and other acts of third parties not under Symantec's control, including wireless carriers, private entities, government entities, and the like ("SMS Network", "Telephone Network", remote notification systems). SYMANTEC SHALL NOT BE LIABLE FOR ANY INTERRUPTION, DELAY, SUSPENSIONS, AND OTHER ACTS AND/OR OMMISSION BY SUCH THIRD PARTIES THAT ARE NOT WITHIN SYMANTEC'S CONTROL.

c. Remedies. In the event that any particular feature within the Service is not Available for reasons other than an Excused Outage and subject to the requirements of Section 3 below, Symantec will provide an extension of the current term of the subscribed service at no charge to Customer in an amount equal to two (2) days of additional service for each 1 hour or part thereof that the service is not available, subject to a maximum of a one (1) additional week of service per incident of un-availability and subject to the maximum of four (4) service extensions for any one year of subscribed service.

c. Chronic Failure. Subject to the requirements of Section 3 below, if the subscribed service is not Available, for reasons other than an Excused Outage, and such non-availability is attributable solely to Symantec and not to Customer, in whole or in part, for more than thirty-six (36) non-consecutive hours in any calendar quarter or where Symantec has provided three (3) or more service remedy extensions for any one year of subscribed service, Customer may terminate the effected service upon thirty (30) days' written notice to Symantec. In the event that Symantec validates the conditions of the termination under this Section, Symantec shall refund to Customer directly or through the reseller, where applicable, a pro-rata portion of the service fees paid in advance and not yet used within forty-five (45) days from termination, or, upon Customer's request and at Symantec's sole option, offer a Service Credit of the pro- rata refund amount toward a new Symantec product purchase to be used within a set period of time.

2. Exclusions.

Notwithstanding any other clause herein, no commitment is made under this policy with respect to: (i) the Service being used in conjunction with hardware or software other than as specified in Symantec's published Documentation; (ii) alterations or modifications to the Service or Service enabling components, unless altered or modified by Symantec (or at the direction of or as approved by Symantec); (iii) defects in the Service due to abuse or use other than in accordance with Symantec's published documentation (unless caused by Symantec or its agents); (iv) an evaluation of the Service or other trial provided to Customer at no charge; and (v) any problems or issues of connectivity due to the network or internet connection of Customer.

No provision of the Agreement will be applicable to VIP pre-production environment availability or performance or Customer test accounts in VIP production environment.

3. Reporting and Claims.

a. To file a Credit Request or termination notice with Credit Request, as applicable, Customer must include in a written notice the following details:
    I. Downtime information detailing the dates and time periods for each instance of claimed downtime during the relevant month (or calendar quarter for termination with a Credit Request).
    II. An explanation of the claim made under this Service Level Agreement, including any relevant calculations.
b. Credit Requests may only be made on a calendar month basis and only for the previous calendar month or part thereof. All Credit Requests must be made within 10 days of the end of each calendar month. A termination notice with a Credit Request must be made within 10 days of the end of a calendar quarter.
c. All Credit Requests will be verified against Symantec's system records. Should any Credit Request submitted by Customer be disputed, Symantec will make a determination in good faith based on its system logs, monitoring reports and configuration records and will provide to Customer a record of service availability for the period in question. The record provided by Symantec shall be definitive. Symantec will provide records of service availability in response to valid Credit Requests upon Customer's request. Symantec shall respond to a Credit Request within 10 days of submission.
d. All remedies referred to in this Service Level Agreement are subject to Customer having paid all applicable fees and fulfilled all of its obligations under the Agreement.
e. Notwithstanding any other clause herein, the remedies in this Service Level Agreement do not apply to any matters arising due to any of the following:
    I. Customer-requested hardware or software upgrades, moves, facility upgrades, etc.
    II. Excused Outages.
    III. Hardware, software or other data center equipment or services not in the control of Symantec or within the scope of the Service.
    IV. Hardware or software configuration changes made by the Customer without the prior written consent of Symantec.

4. Exclusive Remedies.

Notwithstanding any other clause in the Agreement, the remedies set out in this Service Level Agreement shall be Customer's sole and exclusive remedy in contract, tort or otherwise in respect of service affecting events.

24x7 Technical Support and Fault Response

The following applies if Customer is entitled to receive technical Support from Symantec. If Customer is entitled to receive Support from a Symantec reseller, the following does not apply.

- Symantec will on a twenty-four (24) hours/day by seven (7) days/week basis:
    - provide technical support to Customer for problems with the Service; and
    - liaise with Customer to resolve such problems.

For the Support Service Level Agreement, see https://support.symantec.com/en_US/article.TECH236428.html.

EXHIBIT-C

TECHNICAL SUPPORT

- Support is available on a twenty-four (24) hours/day by seven (7) days/week basis to assist Customer with configuration of the Service features and to resolve reported problems with the Service.
- Whenever a Customer raises a problem, fault or request for Service information via telephone or web or portal submission with Symantec, its priority level is determined and it is responded to per the response targets defined in the table below. Faults originating from Customer's actions or requiring the actions of other service providers are beyond the control of Symantec and as such are specifically excluded from this Support commitment.

PROBLEM SEVERITY	SUPPORT (24x7) RESPONSE TARGETS FOLLOWING ACKNOWLEDGEMENT
Severity 1: a problem has occurred where no Workaround is immediately available in one of the following situations: (i) Customer's production server or other mission critical system is down or has had a substantial loss of service; or (ii) a substantial portion of Customer's mission critical data is at a significant risk of loss or corruption.	within 30 minutes
Severity 2: a problem has occurred where a major functionality is severely impaired. Customer's operations can continue in a restricted fashion, although long-term productivity might be adversely affected.	within 2 hours
Severity 3: a problem has occurred with a limited adverse effect on Customer's business operations.	by same time next business day
Severity 4: One of the following: a problem where Customer's business operations have not been adversely affected or a suggestion for new features or an enhancement regarding the Service or Service Enabling Software	within the next business day; Symantec further recommends that Customer submit Customer's suggestion for new features or enhancements to Symantec's forums

Maintenance. Symantec must perform maintenance from time to time. The following applies to such maintenance:

- *Planned Maintenance*. For Planned Maintenance, Symantec will use commercially reasonable efforts to give Customer seven (7) calendar days' notification, via email, SMS, or as posted on the Portal. Symantec will use commercially reasonable efforts to perform Planned Maintenance at times when collective customer activity is low, in the time zone in which the affected Infrastructure is located, and only on part, not all, of the network. If possible, Planned Maintenance will be carried out without affecting the Service. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance in order to minimize disruption of the Service.
- *Emergency Maintenance.* Where Emergency Maintenance is necessary and is likely to affect the Service, Symantec will endeavor to inform the affected parties in advance by posting an alert on the applicable Portal no less than one (1) hour prior to the start of the Emergency Maintenance.
- *Routine Maintenance.* Symantec will use commercially reasonable efforts to perform routine maintenance of Portals at times when collective Customer activity is low to minimize disruption to the availability of the Portal. Customer will not receive prior notification for these routine maintenance activities.

Service Enabling Software. The following applies to Service Enabling Software:

- Symantec will provide software upgrades, bug-fixes, patches, error corrections and enhancements which are developed by Symantec and made available to Symantec's customers for these offerings on an if-and-when-available basis.
- Symantec will provide such customer support as provided in this Service Description only for the then-current release

of the Service or Service Enabling Software and the immediately preceding Minor release of Service Enabling Software at any given time.

Technical Support Contact Information and Telephone Numbers can be found at: https://support.symantec.com/en_US/contact-support.html