STANDARD MAINTENANCE & SUPPORT POLICY

1.0 Maintenance and Support Services

a. SecureAuth Corporation ("SA") shall provide licensees and end users (collectively, "Licensee" or "Customer") maintenance and support services ("Maintenance and Support" or the "Support Services") consisting of bug-fixes, work arounds, corrections, enhancements, updates and new releases and versions of SecureAuth IdP ("Software") made available to customers on a non-beta, commercial basis.

Prior to requesting Support Services, Licensee shall use commercially reasonable efforts to comply with all of SA's published operating and troubleshooting procedures contained in its documentation. Licensee shall use commercially reasonable efforts to gather technical information specific to a problem including Software log files, reports, and error messages. Upon receipt from Licensee of a notice of a Software problem, accompanied by reasonable supporting detail, and expressly provided that the Software problem is then under warranty or a support and maintenance obligation, SA will use reasonable efforts to determine if such Software problem exists and to correct, to the satisfaction of Licensee, such Software problem within the timeframes set forth herein, depending on the severity level of the Software problem.

b. Any corrections to the Software will be made to the most current generally available release of the Software and, if requested by Licensee, to versions N-1 and N-2 of the Software, where version N is the latest listed version at the time. After the introduction of a new and generally available release of the Software, SA will support the then-current and the two (2) prior major releases of such Software. Licensee may install and use all Software updates and enhancements but Licensee is not obliged to do so. SA shall have no obligation to correct any Software problem to the extent of an unauthorized modification or alteration of the Software by Licensee that cause it to deviate from the Documentation, or in the event of operating system or computer malfunction is not caused by the Software. SA will ensure that its API and ID Tool Software, which is part of the licensed Software, will run on Licensee's required operating system and hardware platforms.

c. Licensee acknowledges and agrees that it is, and will be, solely responsible for the accuracy and adequacy of all information and data furnished by Licensee for processing.

1.1. Service Level Overview

SecureAuth agrees to satisfy the service levels set forth in sections 1.1, 1.2 and 1.3 below (the "Service Levels").

a. Service Levels are defined as the measurement of the performance of a service or system.

b. The Service Level target is defined as the percentage or the absolute achievement of that service level goal of which failure to achieve has a noted business impact.

c. SecureAuth's performance with regard to the Service Levels will be measured according to monthly averages, generated for each full calendar month the Services are provided to Customer.

d. Service Level and availability measurements will take effect upon execution of a license agreement by Customer.

e. Service Level measurements will not take in account any agreed upon embargo periods and / or service upgrade outages. Likewise, where the fault or remedial action lies with "Customer" or a third party not affiliated with SecureAuth, measurements will not be applicable for such periods.

1.2 Service Level Requirements

a. Customer Service Levels include two (2) categories: Business Critical and Non-Business Critical. The following table describes the Service Levels target for these two (2) categories:

Service	Description	SLA target
Business Critical	Defined as an application that is essential in the business process. These services are considered core business-critical systems. Their impact is conventionally measured and described in terms of a loss of revenue.	99.9% up time 24 x 7 x 365 days
Non-Business Critical	Defined as an application that is non-essential in the business process. These services are not considered core business systems. Their impact is not measured or described in either terms of lost revenue. Examples of non-business critical items are social media (e.g., Facebook, Instagram, etc.)	99% up time 24 x 7 x 365 days

b. In addition to the foregoing, authentication services availability is subject to the following target Service Levels:

System Component	Target SLA
Services Availability (i.e., SMS, Telephony and Certificate authentication services)	99.9%

1.3. Severity Levels and Response Times

a. Problems reported by Customer or that otherwise come to SA's attention will be logged by SA and assigned a severity level. Response time is the time between when SA is notified of the problem and when SA acknowledges the problem by assigning it a trouble ticket number. Customer shall notify SA at support@secureauth.com or 949-777-6959, ext. 2. Normal support is included with all license subscriptions. Mission critical support is available for all license subscriptions at an additional cost:

The following tables describe the severity levels classification for problems and the expected response time for each problem severity level. SA will respond to problem callouts within the timeframes set forth in the tables below.

	NORMAL SUPPORT				
Severity	**Description**	**Response Time**	**Resolution Target**	**If not resolved, escalated to Tier 3 Support**	**If not resolved, escalated to Director, Support**
Class 1 - Urgent	Coverage: 24 x 7 There is the potential of a health, safety or security issue to occur or it has already occurred. Potential for an operational or financial impact to the business. A Business Critical, Tier 1 system, application or function is completely unavailable, severely corrupted or degraded for more than one authorized user. Note: Severity Level 1 support requests cannot be logged through our support portal; call us to log a severity Level 1 case	1 Hour	N/A	24 hours	24 hours
Class 2 - High	Coverage: A non-business critical system, application or function is unavailable, severely corrupted or severely or degraded for a more than one authorized user.	3 Hours	N/A	5 business days	After 7 business days
Class 3 - Normal	Level 3 is the default severity setting. Coverage: System performance is impaired, but there is no business or “customer” client impact for more than one authorized user.	4 Hours	N/A	7 business days	After 15 business days
Class 4 - Low	A user level fault only affecting one authorized user but not affecting ability to perform business functions – (i.e., no business or “Customer” client impact). Enhancement requests.	24 hours	N/A	14 business days	21 business days

	MISSION CRITICAL SUPPORT				
Severity	**Description**	**Response Time**	**Resolution Target**	**If not resolved, escalated to Tier 3 Support**	**If not resolved, escalated to Director, Support**
Class 1 - Urgent	Coverage: 24 x 7 There is the potential of a health, safety or security issue to occur or it has already occurred. Potential for an operational or financial impact to the business. A Business Critical, Tier 1 system, application or function is completely unavailable, severely corrupted or degraded for more than one authorized user. Note: Severity Level 1 support requests cannot be logged through our support portal; call us to log a severity Level 1 case	30 Minutes	24 hours	Within 5 hours	Within 8 hours
Class 2 - High	Coverage: A non-business critical system, application or function is unavailable, severely corrupted or severely or degraded for a more than one authorized user.	1 Hour	7 business days	Within 3 business days	After 5 business days
Class 3 - Normal	Level 3 is the default severity setting. Coverage: System performance is impaired, but there is no business or “customer” client impact for more than one authorized user.	2 Hours	15 business days	After 7 business days	Within 15 business days
Class 4 - Low	A user level fault only affecting one authorized user but not affecting ability to perform business functions – (i.e., no business or “Customer” client impact). Enhancement requests.	24 hours	On agreed upon schedule	On agreed upon schedule	On agreed upon schedule

1.4 Causes not Attributable to SA

This Maintenance and Support policy does not include services requested as a result of, or with respect to, causes to the extent they are not attributable to SA. Causes which are not attributable to SA include, but are not limited to, the following events caused by Licensee or its agent:

a. Accident; unusual physical, electrical or electromagnetic stress; neglect; misuse; failure or fluctuation of electric power, air conditioning or humidity control; failure of rotation media not furnished by SA; excessive heating; fire and smoke damage; operation of the Software with other media and hardware, Software or telecommunication interfaces not meeting or not maintained in accordance with the manufacturer's specifications; or causes other than ordinary use;

b. Improper installation by Licensee or use of the Software that deviates from any operating procedures established by SA in the applicable documentation; and/or

c. Modification, customization, alteration or addition or attempted modification, customization, alteration or addition of the Software that cause it or deviate from the documentation undertaken by any party other than SA or its agents without the written consent of SA; Software programs made by Licensee or other parties under the control of Licensee.

1.5 Rights and Obligations of Licensee

SA's provision of Maintenance and Support to Licensee is subject to the following:

a. Before production use of the Software, Licensee shall provide SA with an operational architecture document which describes how the Software is being used in the Licensee environment. Documents created as part of the internal support processes of Licensee, which provide all relevant information needed for SA to help troubleshoot problems, are acceptable substitutes;

b. Licensee shall use commercially reasonable efforts to provide SA with reasonably necessary access to the personnel and equipment of Licensee;

c. Licensee shall use commercially reasonable efforts to provide supervision, control and management of the use of the Software. In addition, Licensee shall use commercially reasonable efforts to implement procedures for the protection of information and the implementation of backup facilities in the event of errors or malfunction of the Software or equipment;

d. Licensee shall report all detected errors or malfunctions of the Software to SA. Licensee shall use commercially reasonable efforts to take all steps reasonably necessary to carry out procedures for the rectification of errors or malfunctions within a reasonable time after such procedures have been received from SA;

e. Licensee shall use commercially reasonable efforts to maintain a current backup copy of all programs and data;

f. Licensee shall use commercially reasonable efforts to properly train its personnel in the use and application of the Software; and

g. Licensee may request a written report to monitor its support activity statistics or to verify compliance with the Service Levels. SA will provide such reports within seven (7) business days of the request. Such requests should not exceed once a month.

1.6 Case Registry Contacts

Licensee shall use commercially reasonable efforts to appoint one (1) or more individuals within its organization who is reasonably knowledgeable in the operation of the Software to serve as primary contact between Licensee and SA regarding the registry and report of support calls (the "Case Registry Contacts"). All support inquiries of Licensee shall be initialized through these contacts where possible. As a security precaution, the hotline analyst

may request further information to verify the identity of the caller. If at any point, the hotline analyst believes that the requesting party is not authorized, the hotline may deny any support that could jeopardize the security of the environment until the primary contact(s) are reached. Additionally, any request for improper assistance will be reported to the primary and secondary contacts of Licensee.

1.7 Information Gathering

The Case Registry Contacts should provide SA with a description of the request or problem. To assure accuracy, the hotline analyst may request any of the following information outlined below:

- Name
- Address
- Problem severity
- Problem description
- Exact error messages
- Log information
- Date and time problem was encountered
- Changes made to the configuration/ environment prior to the problem
- Changes made to the configuration/ environment after the problem
- Actions taken to isolate and resolve before contacting the hotline
- Hardware configuration type
- Appliance version release level
- System configuration parameters
- Information about other Software interacting with the Software

1.8 Exclusions. SA provides support and maintenance for its product, SecureAuth IdP, and the appliances on which the product is supplied; provided, however SA does not support, and is no way responsible for any of the underlying or surrounding infrastructure that may be used in conjunction with, or in support of, the SA IdP product by the Customer. The foregoing includes, but is not limited to, the following:

- Identity Stores, including but not limited to. Microsoft Active Directory, Microsoft LDS, OpenLDAP, Novell e-Directory, IBM LDAP, SunOne LSAP, ApacheDS. any other 3rd-party LDAP directories, MS SQL Server, Oracle Server, Google Apps Datastore, and any other identity or profile store.
- Any 3rd party Databases, Datastores, or SIEM products (whether on-premise, or cloud hosted) used for the storage and reporting of any audit, accounting, or reporting data.
- Any underlying hypervisors or hypervisor management products used to host and support the SecureAuth IdP Virtual Appliance, including but not limited to, Microsoft Hyper-V, VMware ESx, and Citrix XenServer.
- Any MDM solutions used to manage any endpoints or mobile devices.
- Any support of endpoint Operating Systems, (including Microsoft Windows, Apple OS X, Linux and Unix Derivatives) and Mobile Operating Systems (including Apple iOS, Android, Windows Mobile/Phone, and Blackberry).
- Any underlying private, or public network infrastructure - both physical and logical.
- Any cloud, or 3rd party hosting services.
- Any 3rd party hardware OTP tokens, proximity cards, and smart cards, and reader devices.
- Any relying party Software, such as those that accept SAML or other assertions from the product.

For the avoidance of doubt, where additional third party infrastructure components are required, SA shall have no liability whatsoever for the third party infrastructure components that may be required to support the use case of Customer.