

SECLORE CLOUD SUPPORT SERVICES AND SLAS

Seclore will provide Support Services (as defined below) for its Services, including services hosted on Cloud and any other AI Services (as defined in Seclore's AI Terms) ("**Services**"), in accordance with the following terms and conditions. For the purposes of this Seclore Cloud Support Services and SLAs (hereinafter referred to as "**Cloud SLA**"), any reference to Seclore or Customer shall mean the respective entities identified in the applicable Agreement and/or Order Form executed between the parties. Capitalised terms used but not defined herein shall have the meanings assigned to them in such Agreement, Order Form, or AI Terms.

A. SCOPE OF SUPPORT SERVICES - The Support Services provided by Seclore will include:

Function	Description
Deployment	Deployment and configuration of the Services in Seclore cloud environment, including role-based access control, cloud virtual network design, and security controls.
Monitoring and upkeep.	Monitoring of the Seclore cloud infrastructure and health of the Services to minimize unplanned interruptions to Services by way of regular internal reviews. Performing capacity planning and reviewing performance metrics of the Seclore cloud environment.
Security	Assess, test, schedule, deploy, and manage patching on Seclore cloud environment. Security controls and hardening, antivirus and malware management, and monitoring to maintain the health of Seclore cloud environment.
Product upgrade	Periodically upgrade the Services with the latest version. Please refer to the Seclore Product Life Cycle Policy for more information.

B. SUMMARY OF SUPPORT SERVICES BY PLAN TYPE (SERVICE WINDOW)

Support Offerings	Standard	Gold
Upgrades / Bug Fixes (Maintenance Releases)	YES	YES
Web Support through support.seclore.com	* 8 x 5	24 x 7
E-mail Support	* 8 x 5	24 x 7
Phone Support	* 8 x 5	24 x 7
Designated Support Contacts **	2	6
Priority Case Routing	Not included	Included
Accelerated SLAs	Not included	Included
Business Reviews & Strategic Planning	Not included	Included

* **Business hours** are defined as 9:00 AM to 5:00 PM in the hosting region (*i.e.*, local time in Mumbai, India and/or Virginia, USA, UAE, and/or Riyadh, Saudi Arabia, as applicable), excluding local holidays and weekends. These times may vary in countries with multiple time zones.

** **Designated Support Contacts:** Designated Support Contacts means named persons in Customer's organization who are authorized to submit tickets to the Seclore support team ("**Seclore Support**") and to work directly with Seclore's support team. Only Designated Support Contacts (*as defined in Section F below*) may submit tickets as well as receive status information with respect to Support Services.

C. Seclore Responsibilities.

- i. **Support Services.** During the Subscription Term, Seclore shall provide Customer with support services in accordance with the support services plan purchased by Customer ("**Support Services**"), as specified on the applicable Order Form. If the Support Services plan is not identified on the applicable Order Form, Customer shall receive the Standard Support Services.
- ii. **Uptime Commitment and Service Credits.**
- a. **Uptime Percentage.** Seclore shall use commercially reasonable efforts to maintain an "Uptime Percentage" of at least ninety-nine and one half percent (99.5%). Subject to the exceptions noted below, Uptime Percentage will be calculated by subtracting from one hundred percent (100%), the percentage of one (1)-minute periods during any calendar quarter (*i.e.*, three (3) calendar months) in which the Services are Unavailable. "Unavailable" or "Unavailability" means that in any one (1)-minute period, Customer is unable to access and/or protect Files. The Uptime Percentage shall be measured by Seclore in accordance with standard industry practices.
- b. **Exclusions from Uptime Percentage.** Notwithstanding anything to the contrary in this Agreement, or elsewhere, any Unavailability issues resulting from or connected to any of the following events will be excluded from the calculation of Uptime Percentage:
- i. any downtime during a planned maintenance window, or resulting from changes to Services requested by Customer,
 - ii. any unavailability caused by circumstances beyond Seclore's reasonable control, including without limitation, acts of God, acts of government, floods, fires, earthquakes, civil unrest, acts of terror, strikes or other labour problems, internet service provider and/or hosting service provider failures or delays, or denial of service attacks,
 - iii. Customer's acts or omissions including, but not limited to, failure of Customer's internet connectivity, Third Party Applications, or any network that is not owned or managed by Seclore.
- c. **Service Credits.** If Seclore does not meet the Uptime Percentage with respect to any particular calendar quarter, then as Customer's sole and exclusive remedy for a breach of Section C (ii), Seclore will provide to Customer a service credit pursuant to the table below ("**Service Credit**"). Service Credits for each quarter can be claimed against future payments to Seclore.

Actual Uptime Percentage	Service Credit
<99.5% but ≥99.0%	5% of Quarterly Fees*
Below 99.0%	10% of Quarterly Fees*

*Quarterly Fees shall mean the annual fees paid by Customer during a Subscription Term, divided by four.

D. UPGRADES

1. Seclore will maintain the Seclore cloud environment and keep it upgraded with latest product releases. There will be a monthly maintenance window every second Saturday of the month where Services availability may be limited or temporarily disrupted.
2. Customer will ensure that Software, if applicable and Seclore Agents are installed and maintained by Users and over-the-air upgrades will be pushed automatically through the Seclore portal as and when new releases are available.

E. USER SUPPORT:

1. Support Levels

Level 1 Support	• Provided by Customer local IT helpdesk
Level 2 Support	• Provided by Application support team of Seclore
Level 3 Support	• Provided by Support seniors/specialist of Seclore
Product Support	• Provided by Product Support group of Seclore
Development Support	• Provided by the product development team of Seclore

2. Customer's local IT helpdesk ("**Helpdesk**") shall be responsible for providing Level 1 Support to Users. Training videos and knowledge bank to provide Level 1 Support will be available on Seclore portal at <http://www.seclore.com/adoption.seclore.com>. The following terms outline Customer's Helpdesk responsibilities:

- i. The Helpdesk will troubleshoot the incident and attempt to provide a resolution to the User.
- ii. In the event Helpdesk is unable to provide a resolution, a Designated Support Contact shall raise a ticket, via the Designated Support Contact, to Seclore's support team, by visiting <https://support.seclore.com/support/home>. Seclore Support will acknowledge the ticket via e-mail and provide a ticket number to the Designated Support Contact.
- iii. In order for Seclore's support team to resolve the incident, the Helpdesk shall document the incident and provide the following details to Seclore's support team (ensuring that it captures enough information to allow Seclore Support to reliably reproduce the error that is the basis for the incident):
 - a. An accurate and complete description of the incident.
 - b. Prioritization of the incident in accordance with Service Priority Definitions set forth in Table A below.

F. DESIGNATED SUPPORT CONTACTS:

- a. Customer shall identify designated support contact(s) and provide Seclore with the following details of such Designated Support Contact(s), which shall be shared with Seclore upon Customer's acceptance of this Cloud SLA:
 - i. Name
 - ii. Designation
 - iii. Email Address
 - iv. Contact Number
- b. Unless otherwise requested by Customer in writing, Seclore will only communicate with Customer's designated support contacts with respect to resolution of support incidents. The designated support contact(s) shall be responsible for providing additional information or remote sessions, as requested by Seclore, to enable Seclore's support team to troubleshoot the incident.
- c. The number of designated support contacts that Customer may appoint is dependent on the level of Support Services Customer has elected. A designated support contact may be changed upon reasonable written notice to Seclore.

G. SERVICE LEVEL COMMITMENTS:

Seclore will respond to tickets based on the Service Priority as defined by Seclore in accordance with Table A below and respond to Customer in accordance with Table B below. Escalation is from the Helpdesk to Seclore's 2nd level support team.

Table A

Service Priority Definitions

Service Priority	Description
Priority 1 (Critical business impact)	Definition: Priority 1 indicates that Customer is unable to use the Services, resulting in a critical impact on business operations. This condition requires immediate resolution. Priority 1 Pre-requisite – A Priority 1 issue has a crippling effect on Customer’s business. i.e., the Seclore Policy Server is down. Key Deliverables – Priority 1 resolution involves reacting to Customer’s emergency by immediately providing an appropriate resource (“Analyst”). Unless another agreement is in place, Priority 1 issues will be serviced on a continual effort basis until the Priority 1 condition has been resolved. Resolution of Priority 1 conditions may include temporary relief, enabling Customer’s business to operate until a more comprehensive solution is provided. Priority 1 resolution shall be subject to the following conditions: • The Services, and the Customer, are eligible for Support Services • Affected functions of the Services must have already been successfully tested by Customer in User Acceptance Testing (“UAT”) and were also working successfully in the past. • The Customer is available, as and when required and on a 24/7 basis, to actively collaborate with the Analyst and provide any information reasonably requested by the Analyst. • Access to Customer’s systems or information about Customer’s systems is available to the Analyst as and when requested, and on a 24/7 basis. • Once an alternative solution or workaround is provided, the Service priority level will be lowered by Seclore at its discretion. Examples of Priority 1 case: • A Policy Server deployed on hosting service provider’s environment or Services deployed in Customer environment has failed. • Multiple Users are unable to access the policy server on hosting service provider’s environment. • The performance of the servers has degraded to an unusable level. • A File is unrecoverable, corrupt, or lost. Examples of cases that are not classified as Priority 1: • The backend database is operational following a one-time outage; root cause analysis is required. • New feature Request or customization

Priority 2 (Significant business impact)	Definition - Priority 2 indicates the Services are usable but severely limited. Priority 2 Pre-requisites: • Services, or a part thereof, are returning an error or not responding. • Degraded performance is negatively impacting business operations, but an acceptable workaround exists. • Once an alternative solution or workaround is provided, the Service Priority level will be lowered by Seclore at its discretion. • Affected Product functions must have already been successfully tested during User Acceptance Testing and were also working successfully in the
	past. Key Deliverables – Priority 2 issues will be resolved during normal business hours, unless otherwise agreed in writing, and until the Priority 2 condition has been resolved. Priority 2 service delivery shall be subject to the following conditions: • Customer is available during normal business hours to collaborate with the Analyst and provides any information reasonably requested by the Analyst. • Access to the Customer’s systems or information about Customer’s systems is available to the Analyst as and when requested, during normal business hours. Examples of Priority 2 case: • Files are taking more time to open than usual. • Customer cannot access the Policy Server Portal. • Users can access Services, but access is slow, sometimes resulting in “page not found” messages or protected files not opening.

Priority 3 (Limited business impact)	Definition – Priority 3 indicates the Services are usable, but some features (which are not critical to operations) are unavailable. Priority 3 Pre-Requisites: • Issue is specific to one or a few Users. • Non-critical bugs are affecting the functioning of certain features. • Customer is able to access all Files. Key Deliverables – Priority 3 issues will be worked on during normal business hours, until the Priority 3 condition has been resolved. Priority 3 service delivery shall be subject to the following conditions: • Customer is available during normal business hours to collaborate with the Analyst and provides any information reasonably requested by the Analyst. • Access to the Customer’s systems or information about Customer’s systems is available to the Analyst as and when requested, during normal business hours. Examples of Priority 3 case: • Questions about how to use the features or functionality. • Feature Enhancement Request. • Usable performance degradation
---	---

Table B

Service Goals and levels by Plan

For the purpose of this Table B, response time shall be defined as the time elapsed between a ticket being raised by the Designated Support Contact and the assignment of a ticket number by Seclore’s support team.

Priority	Initial Incident Targeted Response Time	
	Standard	Gold
P1 (High)	2 Business Hours	2 Hours
P2 (Normal)	8 Business Hours	4 Business Hours
P3 (Low)	3 Business Days	1 Business Day
Services Administration in Seclore Cloud		
System Health Monitoring	24/7	24/7
Uptime Guarantee *	99.5%	99.5%

* Subject to exclusions identified in Section C(ii)(b) of this Cloud SLA.

H. OUT OF SCOPE

1. The following activities are outside the scope of Seclore Support Services:
 - i. Maintenance and Support of the underlying infrastructure in the Customer’s environment or any Third-Party Products (defined below) procured by the Customer on which any Seclore component is installed or integrated with.

- ii. Resolution of issues arising due to problems in the Customer's underlying infrastructure *e.g.*, database issues, network connectivity issues, data loss due to lack of availability of backed-up data, patching operating systems, physical machines, and hardware failure of the servers on which Seclore is installed.
 - iii. Issues arising due to incompatibility with Third-Party Products that are not explicitly supported by Seclore will not be governed by the response timelines mentioned.
2. The following activities are **not** part of Standard Support Services unless explicitly agreed in the Order Form. Such activities will be initiated only as per availability of resources and may be subject to additional charges, such charges to be mutually agreed in writing between Customer and Seclore:
- i. Request for re-training and provision of custom documentation.
 - ii. Request for resolving issues that arise due to improper installation by the Customer's I.T. team, failure to incorporate all upgrades, unauthorized/attempted modification, or alteration not performed by Seclore Support.
 - iii. Onsite Support.
 - iv. Migration of Customer tenant to a different hosting region supported by Seclore.

I. PRODUCT LIFECYCLE, SUPPORT, AND SUNSET

1. Supported versions. Seclore provides support for its software and cloud services on currently supported versions only, as described in [Seclore's Product Life-Cycle Policy and the public Version Lifecycle Matrix](#) (together, the "Lifecycle Documents"). These documents state which versions are supported and for how long.
2. Upgrades instead of backporting: To keep the solution secure and reliable, Seclore delivers new features and most fixes only on the latest minor release of the latest major version. Where an issue is resolved in a supported version, Customer needs to upgrade to that version. Versions that are past their published End-of-Life (EOL) date are not covered by support.
3. Cloud services and customer-installed components: Seclore updates its cloud (SaaS) services for Customer. Where Customer installs agents, connectors, or other components in its own environment, those components must remain on supported versions published in the Lifecycle Documents. Seclore does not guarantee compatibility with, or support for, out-of-support agents or connectors, including where the cloud service has advanced beyond those versions.
4. Third-party products: If the Software or SaaS Offering relies on a third-party product (such as an operating system, productivity suite, database, or directory service) and that third party stops providing generally available support for that product, Seclore's obligation to support the Seclore solution together with that third-party product ends. Customer may need to upgrade or replace such third-party products to continue to receive support.
5. Long-term solution availability: For as long as (a) Customer maintains an active subscription or support agreement and (b) operates on a supported version of the relevant Seclore product family, Seclore will use commercially reasonable efforts to maintain a supported upgrade path within that product family for at least five (5) years from Customer's initial order date. This commitment is at the product family / solution level, not to any specific version, and may require Customer to perform version upgrades during that period.

J. FAIR USAGE POLICY FOR CLOUD HOSTED INFRASTRUCTURE.

Customer's use of the Services is governed by the Fair Usage Policy for the managed Seclore Rights Management infrastructure hosted by Seclore or its hosting service provider. Fair Usage Policy needs to

be adhered to, to ensure that Seclore can provide the agreed service levels, for instance when hosted on a shared infrastructure. Please visit Seclore's [Fair Usage Policy](#) for more information.