EXHIBIT A
ActiveState CVE SLA and Support Services

ver. December 10, 2025

This Exhibit A is subject to and forms part of the ActiveState Master Terms of Service ("TOS"). The CVE remediation commitments described in this Exhibit apply only to ActiveState's Managed Distributions, unless otherwise stated. Standard Support Services and associated Service Level Agreements (SLAs) described below apply only to Customers with a current, paid subscription to ActiveState's Business or Enterprise Products and Services. No support obligations apply to Products or Services made available on Free Tier, including those downloaded or accessed without payment via the ActiveState Platform. Capitalized terms used but not defined in this Exhibit have the meanings given to them in the TOS.

I. Common Vulnerabilities and Exposures ("CVEs")

1. Eligible Fix

ActiveState will use reasonable commercial efforts to address CVEs affecting exclusively ActiveState Managed Distributions, as defined in the ActiveState Master Terms of Service ("TOS"). CVEs will qualify for remediation under this Service Level Agreement ("SLA") if all of the following requirements are met ("Eligible Fix"):

a. The CVE is detected through ActiveState's standard vulnerability monitoring processes and confirmed to affect an ActiveState Managed Distribution..
b. The CVE can be fixed on its own without needing broader changes tied to unrelated bugs
c. If the CVE remediation does not introduce incompatible changes to the project or requires novel work.
d. One of the following conditions is met:
    i. an upstream fix is publicly available and verified by a credible and independent third party to fix the CVE, or
    ii. an affected Managed Distribution can be rebuilt with updated compilers and/or libraries to remediate that CVE; and
    iii. the CVE relates to a Managed Distribution in use and not to any combination with or use of an Ecosystem or Operating System not supported by ActiveState.

www.activestate.com
solutions@activestate.com

2. Severity Scoring.

ActiveState will use the severity rating determined by the Common Vulnerability Scoring System (CVSS") version 3 for an Eligible Fix, further described at https://nvd.nist.gov/vuln-metrics/cvss.

3. Patching.

3.1 ActiveState will make commercially reasonable efforts to patch CVEs in Managed Distributions within the following timeframes, starting from when an Eligible Fix becomes publicly available:

a. Critical Severity: within five (5) business days.
b. High Severity: within ten (10) business days.
c. Medium and Low Severity: within thirty (30) business days.
d. If possible, in the event of a High Impact CVE Event, ActiveState will use commercially reasonable efforts to rebuild the affected Managed Distribution outside of the SLA times.

3.2 A "High Impact CVE Event" means an event in which one or more vulnerabilities affect multiple components simultaneously, requiring remediation in any of the following scenarios:

a. A vulnerability in a single component that is a dependency of many components, such as OpenSSL, requiring all affected components to be rebuilt with special handling, such that an infrastructure change is required (an image or builder), or that twenty percent (20%) or more of the components need to have individual patches to handle the vulnerability from the dependency.
b. Three (3) or more vulnerabilities that require patching simultaneously related to the same root cause.

4. Remediation

A CVE will be considered remediated when any of the following occur:

a. an updated version of the affected Managed Distribution is published to the ActiveState hosted registry,
b. the CVE is no longer detected through ActiveState's standard vulnerability monitoring processes and confirmed to not affect an ActiveState Managed Distribution.
c. the CVE has been clearly marked as fixed in the ActiveState security fixes feed.

www.activestate.com
solutions@activestate.com

In the event a Managed Distribution includes FIPS validated components ActiveState will remediate CVEs as described above, unless remediating would void the FIPS validation.

5. ActiveState Package Catalog

The ActiveState Package Catalog is a curated collection of Artifacts or Components sourced from various Ecosystems, which have been vetted, built, and made available for inclusion in Distributions and Runtimes ("Package Catalog"). ActiveState will make commercially reasonable efforts to remediate CVEs it identifies in the Package Catalog. However, the CVE remediation timelines and service levels described in this document do **not** apply to the Package Catalog.

To address CVEs in the Package Catalog, ActiveState may use one or more of the following methods:

a. Building the affected Artifacts or Components using the latest publicly available version from the corresponding source code;
b. Updating one or more Artifacts or Components to newer versions where applicable.

ActiveState will also take reasonable steps to validate that Package Catalog components continue to work with upstream versions of publicly available packages. However, because the Package Catalog includes modified versions of public available packages, exact functional equivalence is not guaranteed. It is the User's responsibility to confirm that packages from the Package Catalog meet their functional requirements. ActiveState is not responsible for how these packages are used in the User's environment.

II. SUPPORT SERVICES

Upon payment of all applicable Fees to ActiveState and only during the Term of the Order Form, ActiveState will provide the following support services (the "Support Services"):

1. Business Tier Standard Support Services:

The following SLA and support services apply exclusively for Business Tier Services:

ActiveState's will provide email support to a maximum of one named (1) contact Monday to Friday, 8am to 5pm PST, excluding U.S. Federal holidays in accordance with the response times set forth below:

www.activestate.com
solutions@activestate.com

Criteria	Response Time
ActiveState will respond to general inquiries and service related issues by email. ActiveState provides no time commitment on resolution time for fixes/corrections.	2 business day

Support Services inquiries should be addressed to support@activestate.com.

2. Enterprise Tier Standard Support Services

The following support services apply exclusively for Enterprise Tier Services:

- correction of any material Product errors, security or bug-fixes covered by your Authorized Use.
- Remote support for the build, installation, usage, configuration, and diagnosis (dependent on ActiveState's product life cycle) of the Products.

ActiveState's will provide email support at no additional cost to a maximum of two (2) named contacts, additional named contacts can be added for an additional fee, in your organization Monday to Friday, 8am to 5pm PST, excluding U.S. Federal holidays.

Support Services inquiries should be addressed to support@activestate.com:

Severity Level	Criteria	Response Time
1	CRITICAL IMPACT Issues that are product-wide outages, security breaches, or other extreme impacts that require immediate attention	2 business hours
2	SEVERE IMPACT Major issues or feature malfunctions impacting a large number of users or core functions, but not a complete outage.	4 business hours
3	MINOR IMPACT Important but less urgent problems and non-critical features impact.	1 business day

www.activestate.com
solutions@activestate.com

3. ActivePython 2.7 Service Level Commitment

ActiveState will provide the following SLA for ActiveState Platform Managed Distributions of ActivePython 2.7 security fixes:

CVSS Range	ActiveState Classification	Target Time to Resolve from Date of Public Disclosure
9.0 TO 10.0	CRITICAL	3 months (sooner if possible)
7.0 TO 8.9	HIGH	3-6 months
4.0 TO 6.9	MEDIUM	No target resolution time
0.1 TO 3.9	LOW	No target resolution time

"**Date of Public Disclosure**" means the date the Mitre Corporation completes the vulnerability analysis. The above security fix resolution times are only general guidelines that apply to vulnerabilities identified on or after the start date of the Term per the Order Form. Vulnerabilities with Dates of Public Disclosure that pre-exist the start date of the Term of the Order Form may be subject to reasonable extensions in the Target Time to Resolve as determined between the ActiveState and the Customer. Decisions are made in the best interests of ActiveState Customers. Target resolution times are subject to change on a case by case basis guided by an internal risk assessment performed by ActiveState experts. ActiveState may also determine applicability of a specific vulnerability for the customer before providing fixes.

In cases where a security fix is reasonably determined by ActiveState to not be resolvable within the Target Time specified herein, ActiveState will define a commercially reasonable alternative remediation or otherwise elect at its discretion to cease SLA support on that security fix.

4. Restrictions to all Support Services:

ActiveState reserves the right, at its sole discretion, to limit or cancel the Support Services, in whole or in part: (1) for any module, extension, script or other software program that has become obsolete or has been superseded by more recent modules, extensions, scripts or programs or (2) upon the discontinuance of support by the manufacturer of a platform, to limit or cancel support for such platform (the "Archived Platform") upon notice to Customer. In such a case, ActiveState will provide Customer with the most recent stable version of the Products (as distributed regularly from the ActiveState Platform) for the Archived Platform, so long as Customer is current in payment of the Fees.

www.activestate.com
solutions@activestate.com

Customer acknowledges that the Support Services, including that for an Archived Platform, may, at ActiveState's sole discretion, be limited to ActiveState's commercially reasonable efforts and that major fixes may no longer be possible. ActiveState will provide the Support Services solely to Customer's designated contacts for which applicable fees have been paid. ActiveState does not provide the Support Services for software that Customer has modified. For clarity, Customer acknowledges and agrees that ActiveState's sole obligation under this Agreement with respect to any such maintenance and support issue is limited to response and diagnosis of the maintenance and support issue, and such efforts of ActiveState may not render a conclusive "fix" to the maintenance and support issue identified by Customer in all cases. ActiveState will not provide any support services to customer's third-party customers.

www.activestate.com
solutions@activestate.com