

## EXHIBIT A

**EXHIBIT A-1: TECHNICAL SUPPORT**

The following describes the technical support services ("**Technical Support**") that Coupa shall provide for the support level purchased by Customer ("**Support Level**") as stated on the Order Form. The following terms may be updated from time to time, however, for each Order Form, the terms effective as of the execution of the Order Form shall apply for the duration of the applicable Subscription Term.

1. **Scope.** The purpose of Technical Support is to address defects in the Hosted Applications that prevent them from performing in substantial conformance with the applicable Documentation. A resolution to such a defect may consist of a fix, workaround or other relief reasonably determined by Coupa's Technical Support staff.
2. **Online Support Portal.** The Coupa support portal includes an online knowledge base, best practices for use of the Hosted Applications, and a portal for the Designated Support Contacts (as defined below) to submit support tickets.
3. **Live Phone Support.** Support personnel are available to provide Technical Support to Customer, depending on the Support Level (as defined below) purchased by Customer, on the phone, as described at [https://success.coupa.com/Support/Contact\\_Us](https://success.coupa.com/Support/Contact_Us).

4. **Severity Levels.** Each support ticket shall be categorized by Customer into one of the following severity levels.

Severity	Definition
Severity Level 1	Severe error that results in the Hosted Applications experiencing complete unavailability and halting transactions with no workaround.
Severity Level 2	Serious error that results in a major function of the Hosted Applications suffering a reproducible problem causing either major inconvenience to Users or consistent failure in a common functionality.
Severity Level 3	Error that results in a common functionality experiencing an intermittent problem or a consistent failure in a less common functionality.
Severity Level 4	Service requests such as sandbox refreshes, SSO setups, and other how-to type of questions.

5. **Support Levels.** Support personnel will respond to and update each support ticket in accordance with the following timelines.

Support Level	Basic		Premium	
Online Ticket Submission, Phone Support	Severity Level 1: 24x7 Severity Levels 2-4: Mon-Fri, 8am-6pm at Customer's main domicile		All Severity Levels: 24x7	
Designated Support Contacts	Maximum of 5		Maximum of 10	
	Response Times	Update Frequency	Response Times	Update Frequency
Severity Level 1	1 hour	2 hours	30 minutes	1 hour
Severity Level 2	4 hours	1 business day	2 hours	6 hours
Severity Level 3	3 business days	4 business days	2 business days	2 business days
Severity Level 4	7 business days	7 business days	5 business days	5 business days

## 6. Customer Responsibilities

- 6.1. Customer shall designate no more than the number of Coupa Platform administrators ("**Designated Support Contacts**") set forth above who may contact and interact with Coupa in connection with Technical Support requests. Customer's Designated Support Contacts shall answer questions and resolve issues as needed when they arise from other Users of the Hosted Applications. Customer's Designated Support Contacts enter support request tickets, work through Technical Support issues with Coupa, and take action as needed to implement the resolution to the issue. Customer agrees that Coupa may communicate and follow instructions to make changes to Customer Data and/or Customer's instances, with its Designated Support Contacts via email, phone or through the Support Portal.
- 6.2. Customer shall ensure that Customer's Designated Support Contacts are trained on the use and administration of the Hosted Applications. Customer shall ensure that the name, contact and other information for these Designated Support Contacts are current in the Support Portal. Customer may replace Designated Support Contacts by updating the applicable information in the Support Portal, provided that at no time may Customer have more than the number of Designated Support Contacts permitted based on its Support Level.

## 7. Support Exclusions

Coupa is not required to provide resolutions for immaterial defects or defects due to modifications of the Hosted Applications made by anyone other than: (a) Coupa; or (b) Anyone acting at Coupa's direction. Technical Support does not include professional services for implementation, configuration, integration or customization of a Hosted Application or custom software development, training or assistance with administrative functions.

## 8. Update Process

Coupa shall use commercially reasonable efforts to (1) monitor the Hosted Applications and related infrastructure for opportunities to address performance, availability and security issues; and (2) at Coupa's discretion, deliver functionality enhancements to address customer and market requirements to improve such Hosted Applications based on Coupa innovation.

Customer shall comply with the Update Process. Customer understands that Technical Support may not be available if Customer does not comply with the Update Process, and that only the latest release of the Coupa Platform and Hosted Applications contains the most current features, availability, performance and security, including software fixes. Coupa is not responsible for product defects or security issues affecting the Hosted Applications or failure to meet the Uptime SLA (defined in [Exhibit A-2](#)) for Hosted Applications when Customer is not in compliance with the Update Process.

Coupa's update and release process ("**Update Process**"), as updated from time to time, is described at:

Release Types: [https://success.coupa.com/Success/Release\\_Management/01\\_Release\\_Types](https://success.coupa.com/Success/Release_Management/01_Release_Types)

Release Timelines: [https://success.coupa.com/Support/Releases/About/Release\\_Management/02\\_Release\\_Timelines](https://success.coupa.com/Support/Releases/About/Release_Management/02_Release_Timelines)

More Release Info: [https://success.coupa.com/Support/Releases/About/Release\\_Management/08\\_More\\_Release\\_Info](https://success.coupa.com/Support/Releases/About/Release_Management/08_More_Release_Info)

**EXHIBIT A-2: SERVICE LEVEL AGREEMENT (SLA)**

1. If service outages result in a failure of any production instance of a Hosted Application to meet an uptime availability requirement of 99.8% over a calendar month ("**Uptime SLA**"), Customer's sole and exclusive remedy shall be a service credit equal to the *greater* of:
  - (a) Ten percent (10%) of the subscription fees set forth in the applicable Order Form for that calendar month; or
  - (b) The actual unavailability rate for that calendar month (as an example, if the Hosted Application has an uptime availability of 85% during a calendar month, then the service credit shall be fifteen percent (15%) of the applicable subscription fees for that calendar month).
2. The following events shall be excluded in calculating Uptime SLA:
  - (a) Planned maintenance windows, which are described at [https://success.coupa.com?cid=msa\\_planned\\_maintenance](https://success.coupa.com?cid=msa_planned_maintenance)
  - (b) Emergency maintenance required to address an exigent situation with the Hosted Application or Coupa Platform that if not addressed on an emergency basis could result in material harm to the Hosted Application or Coupa Platform. Coupa shall provide advance notice of emergency maintenance via the Support Portal to the extent practicable.
  - (c) Any unavailability caused by circumstances beyond Coupa's reasonable control, including without limitation, unavailability due to Customer or its Users' acts or omissions, a Force Majeure Event, Internet service provider failures or delays, failure or malfunction of equipment or systems not belonging to or controlled by Coupa.

Items (a) – (c) collectively, "**Excused Downtime**".

Coupa reserves the right to perform planned maintenance outside the target periods above if circumstances require, and Coupa shall provide prior notice to Customer via the Support Portal before doing so.

3. Uptime SLA is calculated as follows:

$$\frac{(x - y - z)}{(x - z)} * 100$$

x = total number of minutes in a calendar month

y = downtime that is not excluded

z = Excused Downtime (as defined above)

4. Customer must request all service credits in writing to Coupa within thirty (30) days of the end of the month in which the Uptime SLA was not met, including identifying the period Customer's production instance of the Hosted Applications was not available. Coupa shall apply the service credit during Customer's next billing cycle unless the service credit is reasonably disputed by Coupa, in which case Customer and Coupa shall work together in good faith to resolve such dispute in a timely manner. The total amount of service credits for any month may not exceed the applicable monthly subscription fee for the affected Hosted Applications and has no cash value (unless a service credit is owed at the termination or expiration of this Agreement without a renewal order, in which case, such service credit shall be paid to Customer within ninety (90) days of the end of the Subscription Term). Uptime and other system performance metrics can be found on [trust.coupa.com](https://trust.coupa.com).

**EXHIBIT A-3: DATA SECURITY MEASURES**

The following describes Coupa's Security Program as of the Effective Date. The following terms may be updated from time to time, however, for each Order Form, terms effective as of execution of the Order Form shall apply for the duration of the applicable Subscription Term.

**(A) ORGANIZATIONAL ACCESS CONTROL**

- (i) **Control Environment.** Coupa employees are required to sign a written acknowledgement form documenting their receipt and understanding of the employee handbook and their responsibility for adhering to the policies and procedures therein. Employees are also required to sign a confidentiality agreement agreeing not to disclose proprietary or confidential information, including customer information, to unauthorized parties.
- (ii) **Access Administration.** Coupa employees do not have direct access to Customer Data, except where necessary for Technical Support, system management, maintenance, backups and other purposes separately authorized by Customer in writing. Access to Customer Data is further restricted to technical and customer support staff on a need-to-know basis. When an employee or contractor no longer has a business need for these privileges, his or her access is revoked in a timely manner, even if he or she continues to be an employee or contractor of Coupa. Coupa's policies require Coupa personnel to report any known security incidents to Coupa management for investigation and action.
- (iii) **Personnel Screening.** Criminal background checks are performed for employees with access to Customer Data as part of the hiring process.
- (iv) **Security Awareness and Training.** Coupa maintains a security awareness program that includes training of Coupa personnel on Coupa's security program. Training is conducted at the time of hire and periodically in accordance with Coupa's information security policies.
- (v) **Subprocessors and Data Transfer.** Coupa may engage Subprocessors and other Third-Party Suppliers (each as defined below) to perform some of its obligations under the Agreement. Coupa shall require that Subprocessors only access and use Customer Data in a manner consistent with the terms of the Agreement and bind Subprocessors to written obligations to protect Customer Data. At the written request of Customer, Coupa shall provide additional information regarding Subprocessors and their locations. Customer may send such requests to Coupa's Data Privacy Officer at [legalnotices@coupa.com](mailto:legalnotices@coupa.com). "**Third-Party Suppliers**" means third-party contractors and suppliers engaged by Coupa in the context of the provision of the Hosted Applications or Coupa Platform. "**Subprocessors**" means those Coupa Affiliates and Third-Party Suppliers that have access to, and process, Customer Data. As part of providing the Hosted Applications or Coupa Platform, Coupa and its Subprocessors may transfer, store and process Customer Data in the European Economic Area, United States, India or any other country in which Coupa and its Subprocessors maintain facilities.
- (vi) **Business Continuity Management Process.** Coupa shall maintain a business continuity plan (BCP) that defines the processes and procedures for the company to follow in the event of a disaster and shall review and shall regularly test Coupa's disaster recovery plan to ensure that it is capable of recovering Coupa assets and continuing key Coupa business processes in a timely manner.

**(B) PHYSICAL ACCESS CONTROL**

- (i) **Physical Protection of the Data Centers.** Physical access to data centers is strictly controlled by the data center provider ("**DC Provider**") both at the perimeter and at building ingress points by security staff. The DC Provider only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee or contractor no longer has a business need for these privileges, his or her access is immediately revoked, even if he or she continues to be an employee or contractor of the DC Provider. All physical access to data centers is logged and audited routinely.

- (ii) **Availability.** Data centers are built in various global regions. All data centers are online and serving customers. In case of failure, automated processes move Customer Data traffic away from the affected area. The data centers have backup power and environmental protection systems, which are regularly maintained and tested.
- (iii) **Disaster Recovery.** Coupa shall create a disaster recovery plan designed to provide appropriate technical and operational controls to deliver a recovery time objective (RTO) of typically no more than one (1) day and a recovery point objective (RPO) of typically no more than one (1) hour for the Hosted Applications.
- (iv) **Fire Detection and Suppression.** Automatic fire detection and suppression equipment have been installed to reduce risk and damage to data center environments.
- (v) **Power.** The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Data center facilities have power backup and environmental protection systems in the event of an electrical failure for critical and essential loads in the facility.
- (vi) **Climate and Temperature.** Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.
- (vii) **Monitoring.** The DC Provider monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

(C) **TECHNICAL SECURITY MEASURES**

- (i) **Database Protection.** Database infrastructure is segregated from the application servers and the Internet via firewalls.
- (ii) **Encryption.** All communications are encrypted between the data exporter and the data centers using high-grade encryption (AES-256). Access to Coupa's on-demand applications and services is only available through secure sessions (https) and only available with an authenticated login and password. Passwords are never transmitted or stored in their original form.
- (iii) **Intrusion Protection.** The application infrastructure is protected against intrusion by industry standard protection technology (such as regular penetration testing, firewalls at the network, host, and application levels, and intrusion detection systems) across all servers. Unless otherwise agreed by Coupa in writing, Customer is prohibited from performing its own penetration on any system of Coupa.
- (iv) **Customer Data Isolation.** Coupa Platform services use application or process level segmentation to accomplish data isolation.
- (v) **Malicious Software Protection.** The Hosted Applications and the Coupa Platform shall include reasonably up-to-date versions of system security software (including malware and anti-virus protection).

(D) **EXCLUSIONS**

If Customer installs, uses, or enables third party services that interoperate with the Hosted Applications, then the Hosted Applications may allow such third-party services to access, use, or otherwise process and transmit Customer Data. Coupa's Security Program does not apply to any processing, storage, or transmission of data outside the Coupa Platform, and Coupa is not responsible for the security practices (or any acts or omissions) of any third-party service providers engaged by or on behalf of Customer. The Coupa Security Program excludes: (i) data or information shared with Coupa that is not stored in the Coupa Platform; or (ii) data in Customer's virtual private network (VPN) or a third-party network other than one that is under a subcontract with Coupa to assist Coupa in fulfilling its obligations in the Agreement. Additionally, Coupa shall not be liable for any data (including where part of Customer Data) used, processed, stored or transmitted by Customer or Users in violation of this Agreement.

\*\*\*