**Exhibit B to Sales Order**

**AUTH0**

**PRIVATE CLOUD TERMS**

If Auth0 is required under any Sales Order or Order Form to provide “Private Cloud” Services, then these Auth0 Private Terms Cloud (these “**Private Cloud Terms**”) apply to the Subscription Services provided under the Sales Order or Order Form. These Private Cloud Terms are incorporated into the applicable Sales Order or Order Form, and are subject to the Auth0 Subscription Agreement that applies to the Sales Order or Order Form.

The Private Cloud Terms are as follows:

**“Private Cloud”** means a version of the Auth0 Platform deployed as a private instance for Customer, in a private cloud environment, sourced, operated and managed by Auth0, and dedicated for Customer’s use.

Auth0 will provide the Subscription Services using a Private Cloud. (Details can be reviewed at [https://auth0.com/docs/deploy](https://auth0.com/docs/deploy).)

- **Virtual Machine:** Auth0 will install and manage the Private Cloud on a virtual machine (“**VM**”) provided by Auth0.
- **Root Access; Modification by Customer:** Customer may not utilize root access to the Private Cloud. Customer may not modify or maintain, nor attempt to modify or maintain the Private Cloud, except in accordance with Auth0 instructions.
- **Planning and Administration:** Customer must comply with the Private Cloud requirements specified in the Documentation ([https://auth0.com/docs/private-cloud](https://auth0.com/docs/private-cloud)).
- **Backup:** Backup cycles for Private Cloud subscriptions will be at least the same as for Auth0 public cloud subscription services (currently every 6 hours), except as otherwise mutually agreed in writing between Customer and Auth0.
- **Updates and Patches:** Auth0 does not anticipate requiring any downtime for its installation of updates and patches in production environments.
  - **Private Cloud Basic:** Auth0 will install updates and patches and access the Private Cloud at times determined by Auth0.
  - **Private Cloud – Performance and Performance Plus:** Auth0 will coordinate its installation of updates and patches with Customer. Installation will occur on a regular, periodic basis (generally monthly, but in any event no less than quarterly, and sooner in the case of an emergency such as a required security or performance patch, as commercially reasonably ascertained by Auth0).
- **Update Cadence and Escalations – Private Cloud Performance and Performance Plus:**
  - Auth0 and Customer will work together in good faith to establish a regular update cadence, and will coordinate to determine how to address non-standard circumstances such as general Customer holds on updates across its networks and systems, and Auth0’s need to apply urgent patches. Prior to putting the Subscription Services into production (or as soon as reasonably possible, if the Subscription Services already are in production), Customer and Auth0 will establish an escalation process that enables either party to escalate update issues within the other party’s organization (“**Standard Escalation**”). If either party believes that Standard Escalation has been ineffective, then they may require that each party’s executive sponsors and legal representatives meet via video conference within 5 business days’ of such request (“**Executive Escalation**”).
  - If Customer fails to permit Auth0 to maintain and update their Private Cloud instances for 3 consecutive months or to apply emergency patches to address critical vulnerabilities within 10 days of notification, then Auth0 may escalate using the Standard Escalation procedure. If the issues have not been resolved to each party’s satisfaction within 5 business days of such escalation, then either party may require Executive Escalation. If the issues have not been resolved to each party’s satisfaction within 5 business days of such escalation then, in Auth0’s discretion, Auth0 may terminate the applicable Sales Order or Order Form on not less than 30 days’ prior written notice.
to Customer, and Customer shall not be entitled to any refunds of prepaid amounts to Auth0. Auth0 will not be obligated to provide the Support Program during such 30 day period. Auth0 must withdraw its termination notice if Customer provides Auth0 with access to the Private Cloud for maintenance and update purposes as required by Auth0 within the 30 day period. Auth0 will have no liability for any security breach or service level non-conformance that occurs between expiration of any such 3 month period or 10 day period and Customer’s provision of access to Auth0 for Auth0’s maintenance purposes, nor for any non-conformance by Auth0 with its other obligations under this Agreement that would not have occurred had Customer permitted Auth0 to access and maintain the Private Cloud as soon as reasonably possible following Auth0’s request.

- Without limiting the paragraphs above, if Customer fails to permit Auth0 to maintain and update the Private Cloud instances for 3 consecutive months or to apply emergency patches to address critical vulnerabilities within 10 days of notification, and if, as a result, the Private Cloud version in use by Customer is more than two active releases behind Auth0’s then-current active release, then Auth0 may charge two days’ professional services fees, at its then current rates, for Auth0’s installation of a current release, and Customer will pay such fees for the installation following receipt of invoice, under the payment terms specified in the Subscription Agreement between Auth0 and Customer.