SCHEDULE B

DATA PROCESSING TERMS

The Data Processing Terms (DPT) include the terms in this section. Capitalized terms not set forth herein have the meanings ascribed to them in the Service Agreement.

The Data Processing Terms also include the "Standard Contractual Clauses," pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of Personal Data to processors established in third countries under the EU Data Protection Directive. The Standard Contractual Clauses are enclosed as an attachment to the Data Processing Terms. In addition,

- Execution of the Service Agreement includes execution of Standard Contractual Clauses, which is countersigned by ORock Technologies, Inc. ("ORock");
- The terms in Customer's Cloud Services Agreement ("Service Agreement"), including the DPT, constitute a data processing agreement under which ORock is the data processor; and
- The DPT control over any inconsistent or conflicting provision in Customer's Service Agreement and, for each subscription, will remain in full force and effect until all of the related Customer Data is deleted from ORock's systems in accordance with the DPT.

Customer may opt out of the "Standard Contractual Clauses" or the Data Processing Terms in their entirety. To opt out, Customer must send the following information to ORock in a written notice (under terms of the Customer's Service Agreement):

- the full legal name of the Customer and any Affiliate that is opting out;
- if Customer has multiple Service Agreements, the Service Agreement to which the opt out applies;
- if opting out of the entire DPT, a statement that Customer (or Affiliate) opts out of the entirety of the Data Processing Terms; and
- if opting out of only the Standard Contractual Clauses, a statement that Customer (or Affiliate) opts out of the Standard Contractual Clauses only.

In countries where regulatory approval is required for use of the Standard Contractual Clauses, the Standard Contractual Clauses cannot be relied upon under European Commission 2010/87/EU (of February 2010) to legitimize export of data from the country, unless Customer has the required regulatory approval.

In the DPT, the term "Cloud Services" applies to all ORockCloud Sevices. "Customer Data" includes only Customer Data that is provided through use of those Cloud Services.

Location of Customer Data at Rest

ORock operates a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors operate such facilities. ORock does not control or limit the regions from which Customer or Customer's end users may access or move Customer Data.

Privacy

- **Customer Data Deletion or Return**. No more than 90 days after expiration or termination of Customer's use of an Online Service, ORock will disable the account and delete Customer Data from the account.

- **Transfer of Customer Data**. Unless Customer has opted out of the Standard Contractual Clauses, all transfers of Customer Data out of the European Union, European Economic Area, and Switzerland shall be governed by the Standard Contractual Clauses. ORock will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area and Switzerland.
- **ORock Personnel**. ORock personnel will not process Customer Data without authorization from Customer. ORock personnel are obligated to maintain the security and secrecy of any Customer Data as provided in the DPT and this obligation continues even after their engagement ends.
- **Subcontractor Transfer**. ORock may hire subcontractors to provide certain limited or ancillary services on its behalf. Any subcontractors to whom ORock transfers Customer Data, even those used for storage purposes, will have entered into written agreements with ORock that are no less protective than the DPT. Customer has previously consented to ORock's transfer of Customer Data to subcontractors as described in the DPT. Except as set forth in the DPT, or as Customer may otherwise authorize, ORock will not transfer to any third party (not even for storage purposes) Personal Data Customer provides to ORock through the use of the Cloud Services. ORock maintains a list of ORock Affiliates and Third Party Subprocessors authorized to access and/or process Customer Data in the Cloud Services as well as the limited or ancillary services they provide. At least 3 months before authorizing any new subcontractor to access Customer Data, ORock will update the list and provide Customer with a mechanism to obtain notice of that update. If Customer does not approve of a new subcontractor, then Customer may terminate the affected Online Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval. If the affected Online Service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, ORock will remove payment obligations for the terminated Cloud Services from subsequent Customer invoices.

Additional European Terms.

These Additional European Terms apply only if Customer has end users in the European Economic Area ("EEA") or Switzerland.

- **End Users in EEA or Switzerland**. Terms used in the DPT that are not specifically defined will have the meaning in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data (the "EU Data Protection Directive").
- **Intent of the Parties**. For the Cloud Services, ORock is a data processor (or sub-processor) acting on Customer's behalf. As data processor (or sub-processor), ORock will only act upon Customer's instructions. The DPT and Customer's Service Agreement (including the terms and conditions incorporated by reference therein), along with Customer's use and configuration of features in the Cloud Services, are Customer's complete and final instructions to ORock for the processing of Customer Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer's Cloud Services.
- **Duration and Object of Data Processing**. The duration of data processing shall be for the term designated under Customer's Service Agreement. The objective of the data processing is the performance of the Cloud Services.
- **Scope and Purpose of Data Processing**. The scope and purpose of processing of Customer Data, including any Personal Data included in the Customer Data, is described in the DPT and Customer's Service Agreement.
- **Customer Data Access**. For the term designated under Customer's Service Agreement ORock will, at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide Customer with the ability to correct, delete, or block Customer Data, or (2) make such corrections, deletions, or blockages on Customer's behalf.

Security

- **General Practices**. ORock has implemented and will maintain and follow for the Cloud Services the following security measures, which, in conjunction with the security commitments in the Service Agreement, are ORock's only responsibility with respect to the security of Customer Data.

Domain	Practices
Organization of Information Security	**Security Ownership**. ORock has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities**. ORock personnel with access to Customer Data are subject to confidentiality obligations. **Risk Management Program**. ORock performs a risk assessment before initially processing the Customer Data or launching the Cloud Services service. ORock retains its security documents pursuant to its retention requirements after they are no longer in effect.
Asset Management	**Asset Inventory**. ORock maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to ORock personnel authorized in writing to have such access. **Asset Handling** - ORock does not classify Customer Data. - ORock imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data. - ORock personnel must obtain ORock authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside ORock's facilities.
Human Resources Security	**Security Training**. ORock informs and trains its personnel about relevant security procedures and their respective roles. ORock also informs and trains its personnel of possible consequences of breaching the security rules and procedures. ORock will only use anonymous data in training.
Physical and Environmental Security	**Physical Access to Facilities**. ORock limits access to facilities where information systems that process Customer Data are located to identified authorized individuals only. **Physical Access to Components**. Unless otherwise disclosed by customers, ORock maintains only limited records of the authorized senders/recipients, date and time, and that media is loaded to the Cloud Services. **Protection from Disruptions**. ORock uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal**. ORock uses industry standard processes to delete Customer Data when it is no longer needed.
Communications and Operations Management	**Operational Policy**. ORock maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data. **Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), ORock maintains single or multiple copies of Customer Data from which Customer Data can be recovered based on the particular Cloud Services. - ORock stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located. - ORock has specific procedures in place governing access to copies of Customer Data. - ORock reviews data recovery procedures at least every six months. - ORock logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

Domain	Practices
	Malicious Software. ORock has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks. **Data Beyond Boundaries** - ORock encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks. - ORock restricts access to Customer Data in media leaving its facilities. **Event Logging**. ORock logs, and enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. ORock maintains a record of security privileges of individuals having access to Customer Data. **Access Authorization** - ORock maintains and updates a record of personnel authorized to access ORock systems that contain Customer Data. - ORock deactivates authentication credentials that have not been used for a period of time not to exceed six months. - ORock identifies those personnel who may grant, alter or cancel authorized access to data and resources. - ORock ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers, log-ins and authentication credentials. **Least Privilege** - Technical support personnel are only permitted to have access to Customer Data when needed. - ORock restricts access to Customer Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - ORock instructs ORock personnel to disable administrative sessions when leaving premises ORock controls or when computers are otherwise left unattended. - ORock stores passwords in a way that makes them unintelligible while they are in force. **Authentication** - ORock uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, ORock requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, ORock requires the password to be at least twelve characters long. - ORock ensures that de-activated or expired identifiers are not granted to other individuals. - ORock monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - ORock maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - ORock uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. - ORock may but is not required unless set forth in the Cloud Services, use customer data to enable additional authentication of Users that extends beyond current industry standard practices.

Domain	Practices
	Network Design. ORock has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access.
Information Security Incident Management	**Incident Response Process** - ORock maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the party reporting the breach, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Security Incident, notification by ORock shall be made without unreasonable delay and, in any event, within 5 business days. A "Security Incident" is defined as any unlawful access to any Customer Data stored on ORock's equipment or in ORock's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data. - ORock tracks, or enables Customers to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. ORock security personnel verify logs at least every six months to propose remediation efforts if necessary.
Business Continuity Management	- ORock maintains emergency and contingency plans for the facilities in which ORock information systems that process Customer Data are located. - ORock's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed.

Cloud Services Information Security Policy

Cloud Services and the ORock Base Infrastructure follow a written data security policy ("Information Security Policy") that has been Validated against NIST Special Publication 800-53.

Subject to non-disclosure obligations, ORock will make each Information Security Policy available for review by Customer, along with other information reasonably requested by Customer in writing regarding ORock security practices and policies, all subject to ORock's policies and procedures, which include onsite review**.**

Customer is solely responsible for reviewing each Information Security Policy and making an independent determination as to whether it meets Customer's requirements.

If the Standard Contractual Clauses apply, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the Standard Contractual Clauses.

ORock Audits of Cloud Services
For each Cloud Service, ORock will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data (including Personal Data), as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually for the Cloud Services.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for applicable controls standard or frameworks.
- Each audit will be performed by qualified, independent, third party security auditors at ORock's selection and expense.

Each audit will result in the generation of an audit report ("ORock Audit Report"), which will be ORock's Confidential Information. The ORock Audit Report will clearly disclose any material findings by the auditor. ORock will promptly remediate material findings raised in any ORock Audit Report to the satisfaction of the auditor.

If Customer requests, ORock will provide Customer with access to each ORock Audit Report so that Customer can verify ORock's compliance with the security obligations under the DPT. The ORock Audit Report will be subject to ORock's policies and procedures, including strict non-disclosure and onsite review requirements.

If the Standard Contractual Clauses apply, then (1) Customer agrees to exercise its audit right by instructing ORock to execute the audit as described in this section of the DPT, and (2) if Customer desires to change this instruction, then Customer has the right to do so as set forth in the Standard Contractual Clauses, which shall be requested in writing.

If the Standard Contractual Clauses apply, then nothing in this section of the DPT varies or modifies the Standard Contractual Clauses or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.