1. DEFINITIONS

"API" means Application Program Interface which is a set of routines, protocols, and tools for building software applications.
"API Banking Services" means the Services (including associated APIs), Content, RBL Bank marks, and any other product or service provided by RBL Bank under these Terms and Conditions. Service does not include Third-Party Content including those transactional/ non-transactional/ regulatory and/or governance related APIs made available by RBL Bank under this Terms and Conditions and as more particularly described in set up form, ancillary documents and schedules attached hereto.
"API Data" means any data or other content that may be made available by RBL Bank.
"App" means any software application that Client has developed, or intend to develop, through the use of an API.
"Authorized Personnel" means the list of authorized signatory as more particularly described in board resolution submitted along with the set up form submitted by the Client hereto for the said Services and who shall be entitled on behalf of the Client to provide instructions/ approvals to RBL Bank in relation to the API Banking Services availed.
"**Bank**" or "**RBL Bank**" or "**RBL**" means RBL Bank Limited.
"Content" means Content of RBL or any of its affiliates, service providers and sub-contractors, made available in connection with the Services to allow access to and use of the Services, including APIs,, Documentation, sample code, software libraries, command line tools, proof of concepts, templates, and other related technology (including any of the foregoing that are provided by RBL Bank's personnel).
"**Client**" any legal person and its authorised representatives, employees, Personnel, contractors, agents and sub-contractors utilizing the API services extended by the Bank.
"Client Content" means Content that the Client or any Client End User transfers to RBL for processing or storage in connection with the API Banking Services and any computational results that Client or any Client End User derive from the foregoing through Clients use of the Services.
"**Data Protection Legislation**" means the legislation and regulations relating to the protection of Personal Data and processing, storage, usage, collection and/or application of Personal Data or privacy of an individual including (without limitation) any other Applicable Law solely relating to the protection of Personal Data and processing, storage, usage, collection and/or application of Personal Data or privacy of an individual.
"Data Set" means any data set forming part of the API Data
"Documentation" means the user guides and admin guides (in each case exclusive of content referenced via hyperlink) for the Services through RBL Bank Developer Portal (and any successor or related locations designated by RBL Bank), as such user guides and admin guides may be updated by RBL Bank from time to time.
"End User" means any individual or entity that directly or indirectly through another user: (a) accesses or uses Client Content; or (b) otherwise accesses or uses the Service under this Terms and Conditions using Client credentials.
"**RBL Bank Developer Portal"** refers to the online portal which RBL Bank may make available from time to time to enable access to APIs for application development relating to publicly available data.
"**Personal Data**" shall have the same meaning as ascribed in Data Protection Legislations as amended from time to time.
"API Services" means a Service made available by RBL Bank, which is a software intermediary that allows two applications to interact with each other and serves as an interface between different software programs and facilitates their interaction. APIs provide a standard way of accessing any application data, or device, whether it is accessing cloud applications like Salesforce, or shopping from your mobile phone.
"Suggestions" means all suggested improvements or changes to the Service that the Client provide to us.
"Third-Party Content" means Content made available to the Client at the request of the Client by any third party through Bank's Service offering or in conjunction with the Services.

2. TERMS OF USE OF SERVICES BY CLIENT

The Client must conform to RBL Bank's requirements in respect of the technical specifications mentioned in the API portal, as the case may be. RBL Bank disclaims any liability that may arise in connection with any interception of or interference with such information or instruction that has not been encrypted by the Client or at the direction of the Client.

3. CONSIDERATION

RBL Bank shall be entitled to Charges ("Service Fees") as provided in the Commercial Offer Letter and Client shall ensure timeline payments of the same. RBL Bank reserves the rights to revise the Service Fees from time to time. Such revised Service Fees shall be effective upon RBL Bank giving the Client 15 (fifteen) days' of notice in writing.

4. INTELLECTUAL PROPERTY

RBL Bank or RBL suppliers, service providers and sub-contractors own all rights, title and interest (including any intellectual property rights) in and to the RBL Bank API Portal (including any content on it, other than Clients Content), the APIs ,API Data, Data Sets and all other software and systems used by RBL Bank. Client must not use any trademarks, logos or brands of RBL Bank without the Service. express written approval of the Bank. Neither the Client nor any End User will use the Service Offerings in any manner or for any purpose other than as expressly permitted by these Terms and Conditions. Neither the Client nor any End User will, or will attempt to (a) modify, distribute, alter, tamper with, repair, or otherwise create derivative works of any Content included in the Service Offerings, (b) reverse engineer, disassemble, or decompile the Service Offerings or apply any other process or procedure to derive the source code of any software included in the Service Offerings, (c) access or use the Service Offerings in a way intended to avoid incurring fees or exceeding usage limits or quotas, or (d) resell or sublicense the Service offerings. Client represents and warrants that the Bank has the right to use, reproduce, transmit, copy, display and distribute Client's Content. The Client grants RBL Bank the license to use and copy Client's content and that such use will not violate or infringe the rights (including intellectual property rights) of any third party. Client agrees and confirms that subject to the terms of these Terms and Conditions, RBL has granted the Client a limited, revocable, non-exclusive, non-sub licensable, non-transferrable license to do the following: (a) access and use the Services solely in accordance with these Terms and Conditions for its own internal consumption; Client obtains no other rights under these Terms and Conditions to the Service, including but not limited to any related intellectual property rights.Client shall comply with any and all guidelines issued by the Bank regarding use of the Bank's trademarks, logos or brands. The Bank may, at any point of time, without cause, revoke any approval provided for use of the Bank's trademarks, logos or brands. Nothing in these Terms and Conditions grants or transfers to the Client any intellectual property rights or other interest in any of the Bank's trademarks, logos or brands or in any other form of intellectual property of the Bank.

Suggestions: If Client provides any Suggestions to RBL or RBL affiliates, service providers, suppliers or sub-contractors, RBL Bank will be entitled to use the Suggestions without restriction. The Client hereby irrevocably assigns to RBL all right, title, and interest in and to the Suggestions and agree to provide RBL any assistance RBL requires to document, register, and maintain RBL Banks rights in the Suggestions.

5. CONFIDENTIALITY AND DATA PROTECTION

During the course of consumption of API Banking Services, the Client may have access to confidential or proprietary information regarding RBL and related business entities (the "Information"). Client acknowledges the proprietary and sensitive nature of the Information, and the importance of maintaining the secrecy and confidentiality of such Information. Client shall ensure that Information shall be segregated from other information in possession of the Client. Client agrees to implement security conformity requirements as detailed under Annexure-I that are designed to safeguard Information of RBL and shall at all times have appropriate technical and organizational measures in place. All Information accessed including but not limited documents and data, shall belong to RBL absolutely and Client shall, deliver the same forthwith upon request. Client (i) shall not, without RBL's prior written consent, disclose the Information in any manner to any third party (ii) shall treat Information with at least the same degree of care that it treats its own confidential information, but in no event with less than a reasonable degree of care. Client shall notify RBL immediately of any loss or unauthorized disclosure or use of Information that comes to its attention. Upon demand, or upon the termination of these Terms and Conditions, Client shall comply with RBL's instructions regarding the disposition or return of the Information in its possession or control.

The Client shall comply with all Data Protection Legislation as maybe required under Applicable Laws. The Client shall only undertake the processing of Personal Data that is reasonably required in connection with the permitted purpose; and in accordance with the RBL written instructions. The Client shall comply with all reasonable procedures and processes notified by RBL from time to time. The Client shall not process or transfer any Personal Data outside India without the prior written consent of RBL. .On RBLs reasonable request, the Client will provide a detailed, written description of the measures undertaken by the Client and the Clients compliance with those measures and allow RBL to access to the Clients premises to inspect its procedures for the processing of Personal Data; Upon expiry or termination of these Terms and Conditions for any reason the Client shall immediately return, or at RBLs option, destroy any Personal Data held by it or its sub-contractors. Personnel or subcontractors of the Client and issue a confirmation of compliance in this regard to RBL. The Client consents are agrees that any Personal Information, if any, provided by the Bank by virtue of the Services mentioned in these Terms and Conditions shall not be transferred outside the territorial jurisdiction of India.

6. AUDIT AND INSPECTION

On receipt of a reasonable notice from RBL, the Client shall provide access to and make available to any of RBL's officers / employees/ management or internal / external auditors/regulators of RBL, the necessary records for inspection / examination / audit, and co-operate to the fullest extent so as to clarify on any activities and to assure a prompt and accurate audit. The Client shall keep complete and accurate records of all operations in connection with the Services. All said records shall be kept on file by the Client for a period as required under Applicable Laws, and in any event, shall not be excised without first having duly and adequately and timely informed RBL.

7. MISCELLANEOUS

i. Client shall not use the name, trademark or logo of RBL in any sale, marketing publication, advertisement, or other publication and shall not make, or let its employees, agents or subcontractors make, any public statement relating to RBL without prior written consent of RBL.

ii. The API Banking Services shall not be available if prevented due to Force Majeure events such as factors including but not limited to civil commotion, sabotage, lockout, strike or other labour disturbances of any kind interfering with or affecting the normal functioning of Bank or of the Platform , accidents, fires, flood, explosion, epidemic, quarantine restrictions, damage to Bank's and/or the Bank's vendors' facilities, absence of the usual means of communication or transportation, or factors leading to the unavailability of the Internet for the Bank and/or the Client, or computer hacking, unauthorized access to computer data and storage devices, computer crashes, or any other cause, whether of same or a different nature, unavoidable or beyond the control of the Bank.

iii. The waiver or modification by either Party of any term or condition of these Terms and Conditions shall not void, waive, or modify any other term or condition of these Terms and Conditions. The failure of either Party to insist, in any one or more instances, upon the performance of any term of these Terms and Conditions shall not be construed as a waiver or relinquishment of such Party's right to such performance or to future performance of such item. A waiver granted on one occasion shall not constitute a waiver of any future occasion.

iv. Client shall not, directly or indirectly, assign these Terms and Conditions or any of its rights or obligations under these Terms and Conditions without the prior written consent of the Bank. Bank is hereby authorised to assign or sub contract any of its rights, benefits, duties & obligations under these Terms and Conditions without prior consent of the Client.

v. Neither the Client nor any of its related parties, associate companies (as defined in the Companies Act, 2013 amended from time to time) or Client affiliates shall or has ,in relation to the transactions the subject of these Terms and Conditions or otherwise made, offered or authorized or will make, offer or authorize any payment, gift, promise or other advantage, whether directly or through any other person or entity, to or for the use or benefit of any government official or any entity or other person where such payment, gift, promise or other advantage would violate the anti-bribery, anti-corruption and money-laundering laws and obligations or any other applicable Law as maybe enacted from time to time.

vi. Sections on Consideration, Intellectual Property Rights, Indemnity, Disclaimer, Limitation of Liability, Miscellaneous will continue to apply in accordance with their terms and shall survive termination.

vii. These Terms and Conditions, together with all annexures / schedules, constitutes the full and complete understanding of the parties with respect to the subject matter of these Terms and Conditions and constitutes a full statement of the terms of these Terms and Conditions. These Terms and Conditions supersedes all prior written agreements and contemporaneous oral agreements between the parties with respect to the subject matter of these Terms and Conditions, neither party has relied upon any representation of the other not set forth herein as an inducement to enter into these Terms and Conditions.

SECURITY CONFORMANCE REQUIREMENTS

Sr. No.	Control Section	Control Statements & Guidelines
1	Identity Management	All Users only have access to the credentials on a need-to-have basis.
2		The passwords should are not shared amongst users. Users individually have their own unique credentials.
3		The passwords/Secret Key and the API Password are used judiciously and cautiously so that unauthorized users/systems do not have access to these credentials under any circumstances.
4		The systems have an authentication mechanisms including but not limited to an unique username/password combination for login for each user.
5		Password security is enforced with the minimum of the below listed parameters: Minimum Password length of 8 characters. Lower and Upper cases compulsory. Complexity with alpha-numeric & one special character & one capital character. Password expiry – 30 days. Password history – 5. Minimum age of password – 1. User should be able to change the password. Old password should be asked while changing the password. Password cannot be username or any portion of user ID.
6		Users are temporarily locked after specified number of unsuccessful attempts and have to have their account manually reset.
7	Infrastructure Management	Client machines are secured with anti-virus/anti-malware solutions. The Client shall ensure that any software or API or integration from Client end with RBL is free of any back door, drop dead device, time bomb, trojan horse, virus, worm, spyware or adware (as such terms are commonly understood in the I.T. industry) or any other code designed or intended to have, or capable of performing or facilitating, any type of disruption, disablement, harm, impede in any manner the operation of, or providing unauthorized access to, a computer system or network or other device on which such code is stored or installed. Client shall implement measures designed to prevent the introduction of any malicious code into RBL systems, including firewall protections and regular virus scans.
8		Data Leakage Prevention controls are deployed to ensure information doesn't get leaked out of the environment.
9		Security technologies like Firewalls/IPS/WAF/PIM/SIEM/APT are implemented to protect the infrastructure for internal and external security breaches and attacks.
10		Audit Trails should be enabled across the environment for security event and incident logging and monitoring.
11	Security Policy	Client has an Information security policy, which is approved by the management, published and communicated as appropriate to all employees.
12		The Information security policy includes a management commitment and sets out the organizational approach to managing information security.
13		Risk assessments are carried out on a periodic basis
14		The controls are identified in risk assessment procedures
15		There are regular onsite reviews of the outsourced operations
16		The implementation of security policy is reviewed independently on regular basis.

17		There is continuous awareness programmes are conducted for security awareness.
18		There is a confidentiality clause in the terms and conditions and in the contracts with employees/staff/partners/third parties, etc.
19	Physical Security	There are Access control mechanisms deployed (e.g. card swipe systems, biometrics etc.)
20		Access to the computer room(s) limited to approve personnel only
21		There are entry controls are in place to allow only Authorized Personnel into various areas within the organization
22		There are entry and exit points monitored either by guards or cameras.
23		There are Periodic reviews of physical access permissions
24		There is ongoing monitoring of computing facility
25		The control of visitors is adequately addressed
26		In case of outsourced software, all maintenance work is carried out only in the presence of / with the knowledge of appropriate staff
27		The parameters to control the password format have been properly set according to security policy stipulated by the Bank
28		The Information processing service is protected from natural and man-made disasters
29		The delivery area and information processing area are isolated from each other to avoid any unauthorized access?
30		The information is only available on need to know basis.
31		There are security controls for third parties or for personnel working in secure area
32		There are controls adopted to minimize risk from potential threats such as theft, fire, explosives, smoke, water, dust, vibration, chemical effects, electrical supply interfaces, electromagnetic radiation, flood., which could adversely affect the operation of information processing facilities
33		The rooms, which have the Information processing service, are locked or have lockable cabinets or safes.
34		The equipment is protected from power failures
35		The storage device containing sensitive information are physically destroyed or securely over Written.
36		The disposal of sensitive items are logged where necessary in order to maintain an audit trail
37		The equipment, information or software cannot be taken offsite without appropriate authorization
38	Information Handling	There is a documented process for immediate disabling or modification of access entitlements when an employee status changes (termination, transfer, etc.)
39		There are sufficient controls to ensure that the information is handled, processed, stored, accessed in a secured manner
40	Business Recovery	There is a documented business recovery plan
41	Operations Management	There is a secure backup procedures that have been defined and followed
42		All programs running on production systems are subject to strict change control

43		There is an Incident Management procedure exists to handle security incidents
44	SLA Management	Appropriate SLAs have been defined to monitor and review the activities as per the defined agreements for timelines
45	System Management	There are 24x7 alerting and monitoring process in place
46		There is a segregation of duties between roles. E.g. developers do not have administration responsibilities for live services.
47		Roles and responsibilities clearly documented
48		Audit trail for administrator access are maintained. These audit trails are subjected to independent review.
49	System Security	Access to audit trails is restricted
50		High privileged accounts e.g. root only used under change control procedures and not for day-to-day system operation.
51		Security vulnerability management process in place and documented (including but not limited to Application Security Testing, Vulnerability Assessment, Penetration Testing, Hardening, etc.
52		Patch management procedure in place
53	Network Management	The Client has a 'default deny and implicit drop stance' that forces systems fail closed and dropping all traffic not expressly permitted
54		There is a network firewall in place
55		Extra Security is in place for wireless LAN technology
56		There are on-going vulnerability and penetration assessments performed on all servers on a regular basis and appropriate actions taken to remove vulnerabilities
57		UAT/Development/Production environments is segregated from each other using strict access controls over the firewall
58	Personnel Security	Verification checks on permanent staff were carried out at the time of job applications.
59		Reference checks done for the employees
60		There are enhanced screening processes for staff/managers in particularly sensitive roles
61		Employment contracts include: - Confidentiality clauses - Reference to security responsibilities - Penalties / disciplinary proceedings for non-compliance
62		There is an exit process for revocation of physical & logical access permissions
63		All employees/staff/outsourced staff within the organization and third party users (where relevant) receive appropriate Information Security training and regular updates in organizational policies and procedures

64		There is a formal disciplinary process in place for employees who have violated security policies and procedures or guidelines for users, to report security weakness in, or threats to, systems or services

****