INFORMATION SECURITY STANDARDS SCHEDULE

This Information Security Standards Schedule ("Schedule") is made part of, and is hereby incorporated by reference into, the Order Form between the parties. All capitalized terms not otherwise defined herein shall have the meanings ascribed to them in the Agreement. In the event of any conflict between the Order Form and this Schedule, this Schedule shall govern.

1. INFORMATION SECURITY PROGRAM.

1.1 Moody's has established and maintains a comprehensive written information security program that implements reasonable administrative, technical and physical safeguards intended to (i) protect Business Data from unauthorized access, disclosure, use, modification, loss or destruction; (ii) protect against any anticipated threats to the confidentiality, security or availability or integrity of the Business Data; and (iii) properly and securely dispose of the Business Data in accordance with industry standards. Moody's may modify its information security program from time to time, provided that such modifications, either individually or in the aggregate, will not materially reduce the overall level of protection for Business Data. Moody's maintains its information security program and applicable safeguards at all Moody's sites at which an information system that stores or otherwise processes Business Data is located. As used herein, "Business Data" means electronic information submitted by Authorized Users to or through the Products for storage or processing, and all derivatives of such data.

1.2 Moody's physical security measures will include securing business facilities and data centers, and all paper files, servers, back-up systems and computing equipment contained therein. Moody's will maintain commercially reasonable physical security controls at all facilities at which an information system that stores, accesses or otherwise processes Business Data is located. Moody's appropriately restricts physical access to such facilities and information systems. Physical access controls have been implemented for all data centers where Business Data is stored, including 24x7 onsite staff, biometric scanning, and security camera monitoring on entry doors. Data center physical security is audited by an independent firm.

1.3 Moody's information security program will require the following: (i) segregation of Business Data from information of Moody's or its other customers so that Business Data is not commingled with any other types of information, (ii) encryption, using industry standard encryption tools, of all records and files containing Business Data that Moody's (A) transmits or sends wirelessly or across public networks; (B) stores on laptops or removable storage media; (C) where technically feasible, stores on portable devices; and (D) stores on any device that is transported outside of the physical or logical controls of Moody's; (iii) safeguarding of the security and confidentiality of all encryption keys associated with encrypted Business Data; (iv) implementation of processes and procedures intended to authenticate, monitor and report on access to and use of Business Data; (v) processes, procedures and technology intended to maintain network security and to detect a breach or other failure of such security measures, such processes and procedures to include, among other things, (A) access controls, (B) firewalls; (C) audit logs and monitoring reports that are designed to identify unauthorized activities, detect intrusions, reconstruct events and promote accountability by any and all persons who access or use Business Data, (D) restricted access privileges, and (E) a written incident response plan; (vi) ensuring its information systems and associated technologies are monitored by authorized personnel to detect intrusions and unauthorized activities; and (vii) multi-factor authentication for all individuals accessing Moody's internal networks from an external network.

1.4 If Moody's is using or supplying devices or other technology assets in the performance of Products and Services to Client, Moody's must, where applicable, have documented standards and procedures to ensure such are appropriately secured prior to deployment, including complying with the following requirements: (i) devices must be running supported firmware provided by the applicable manufacturer; (ii) access to device firmware or BIOS must be protected by password where available; (iii) network ports, services and protocols that are not used or are prohibited by policy must be disabled; (iv) applicable security and vulnerability management software must be installed, including, but not limited to, anti-virus, firewall, log collection, intrusion prevention and software patching; (v) logging of security events is enabled and at a minimum, logging must capture access policy changes, software installation/updates, failed logins and the creation of accounts with elevated privileges; security event logs must be retained for at least ninety (90) days; (vi) default passwords for built-in administrative accounts must be changed and must comply with strong password requirements, and built-in administrative accounts should be renamed where practical; and (vii) guest and anonymous account access must be disabled unless required for device operation.

2. Asset Management. Moody's has implemented policies and procedures to identify, classify and manage information assets, including both software and hardware assets, and their designated owner. Moody's performs regular asset inventories. Moody's has processes to classify data and identify sensitive, valuable and critical data that Moody's stores, processes or transmits.

3. Personnel Security. Moody's has clearly defined roles and responsibilities for employees, including with respect to information security. In accordance with applicable laws to Moody's and its provision of its Products and Services to its customers, Moody's conducts appropriate and thorough pre-employment screening to protect against security-related or other potential risks presented by personnel. Moody's will only allow persons to have access to Business Data who have undertaken background security checks of a type and scope that are normal and customary for the financial services industry and comply with applicable laws. Such background checks shall include address and employment history verification, the right to work in the relevant jurisdiction, screening against databases of individuals subject to economic sanctions and, if permitted by applicable laws, criminal records checks. Moody's will exclude any of its personnel from accessing the Business Data (i) whose background check reveals they have been convicted of any criminal offense involving dishonesty or breach of trust, including money laundering or any criminal offense concerning the illegal manufacture, sale or distribution of or trafficking in controlled substances, (ii) who appear on any sanctions database or (iii) who are not authorized to work in the relevant jurisdiction.

3.1 *Confidentiality Obligation.* Moody's imposes confidentiality obligations on its personnel who will be provided access to, or will otherwise process, Business Data, including the obligation to protect Business Data in accordance with the requirements of this Schedule (including during the term of their employment or engagement and thereafter).

3.2 *Information Security Training and Awareness.* Moody's implements a security awareness program to train personnel about their security obligations, including in relation to information classification and handling, acceptable use, physical security controls, best practices, and security incident reporting, as well as training product personnel on secure application development.

3.3 *Disciplinary Actions.* Moody's has formal disciplinary processes that apply in the event that any personnel violate their confidentiality or other information security obligations in relation to Business Data.

4. Software Vulnerability Management. Moody's defines and maintains standards for patch management, and vulnerability management designed to ensure that software on any of Moody's assets is regularly updated to mitigate security gaps, including addressing the following: (i) periodic vulnerability scans on all Moody's systems that host, access or otherwise process Business Data; (ii) identification of software that will be updated; include all software components (i.e., client, server and database) where appropriate; (iii) identification of authorized source(s) for the software updates; and (iv) maintaining a process for authorizing and tracking software patching exceptions. The scope of the software vulnerability management program shall also cover security software (e.g., anti-virus and anti-malware), which shall be installed and enabled on each host that is capable of running such software and on gateways, and Moody's shall ensure that the scanning engine and signature or pattern files are kept current; and block access to known malicious domains.

5. Application Security. Moody's maintains a security software development program that includes the use of (i) industry best practices that are in compliance with OWASP principles and, conducts regular application security testing; and (ii) third-party penetration testing. Upon Client's request, Moody's will make available to Client up to once per year a copy of a penetration testing executive summary report, if Moody's has conducted penetration testing for the applicable services. Except as set forth in the Agreement, Moody's must support any production hardware or software used in connection with or which form part of the Products and Services, including updates to address known security flaws and vulnerabilities, in support of which, Moody's maintains internal timeframes for vulnerability remediation in accordance with Moody's internal policies.

6. Change Management. Moody's is responsible for implementing system change management procedures ensuring that any system modifications affecting the

Products and Services are consistent with the Moody's information security program and other security requirements specified in this Schedule.

7. Access Control. Moody's maintains policies and procedures that define the requirements for access to information, including approvals, onboarding and off-boarding requirements, password requirements, segregation of duties, periodic user access recertification, and the logging/monitoring requirements and mechanisms.

7.1 Only authorized personnel can grant, modify or revoke access to an information system.

7.2 All personnel are assigned unique user IDs.

7.3 Access rights are implemented adhering to the "least privilege" approach.

7.4 Moody's implements commercially reasonable password management requirements, including in relation to password length, complexity, expiration, and reuse.

7.5 System access for terminated personnel is promptly removed.

8. Control of Media. When media are to be disposed of or reused, procedures have been implemented to prevent subsequent retrieval of any Business Data stored on them before they are withdrawn from the inventory. When media are to leave the premises at which the files are located as a result of maintenance operations, procedures have been implemented to prevent undue retrieval of Business Data stored on them.

9. Third Party Risk Management. Moody's maintains a Third Party Risk Management program that involves review of the information security practices and controls of subcontractors and, as necessary, required remediation and monitoring of each such subcontractor's control gaps.

10. Incident Response. Moody's maintains an Incident Response Plan that includes incident handling responsibilities and delegation of authority, and guidelines for forensics, evidence collection, post incident review, reporting, and testing. Moody's reviews this plan at least annually considering organizational changes, past incidents, current and emerging threats and other factors. Moody's also performs tabletop exercises to test the teams and their processes, and to identify any gaps in the plan or associated response scenarios. Moody's will provide notice to Client no later than 72 hours after Moody's becomes aware of an incident of unauthorized access to Business Data. The notice shall contain the following: (i) a description of the incident, (ii) the type of information subject to the unauthorized access, and (iii) the measures taken by Moody's to protect Client from further unauthorized access.

11. Audit. Upon Client's request, Moody's will make available to Client up to once per year a copy of a third-party assessment, such as an SOC (System and Organization Controls) report or comparable report ("Third-Party Report"), if Moody's has obtained such a Third-Party Report for the applicable services.

12. Business Continuity and Disaster Recovery. Moody's shall maintain throughout the provision of Products and Services an appropriate disaster recovery and business continuity plan (the "BCP") in compliance with applicable laws and consistent with industry standards. Moody's reviews its BCP and risk assessment regularly. The BCP is tested and updated regularly to ensure that it is up to date and effective. Upon Client's written request, Moody's will furnish Client with an executive summary of the BCP, including operating procedures, integrity of service, test objectives and results of annual tests of the BCP. Moody's will use commercially reasonable efforts to modify the BCP as needed to comply with changes in legal or regulatory requirements and industry standard.