CoreLogic Rental Property Solutions, LLC, ("RPS")

Screening Service Agreement
Policies and Procedures
Applicable to End Users

In order to comply, and ensure Client's corresponding compliance, with Applicable Laws, rules, regulations, and requirements imposed on RPS by TransUnion, Equifax, Experian, other consumer reporting agencies, third party vendors, and data service providers, RPS will strictly enforce RPS's Policies and Procedures as set forth herein, which form a material part of the Screening Service Agreement between RPS and Client ("Agreement"). If the Policies and Procedures conflict with the Agreement, the provisions of the Agreement shall govern and control

RPS's Policies and Procedures can be changed by RPS, in its sole discretion, from time to time based on Applicable Laws, rules, regulations, agreements with RPS's vendors and data services providers, practices in the consumer reporting industry, and for other reasons considered appropriate by RPS. In the event of Client's failure to comply with these Policies and Procedures, RPS will exercise its remedies as set forth in the Agreement. **It shall be solely Client's responsibility to ensure that it is in full compliance with Applicable Laws rules, regulations, and all of RPS's Policies and Procedures before requesting or using any Consumer Report Information**.

I. Roles & Responsibilities

A. RPS ROLE

CoreLogic Rental Property Solutions, LLC (RPS) is a Consumer Reporting Agency (CRA) as defined by §603(f) of the Fair Credit Reporting Act (the FCRA) and thus is subject to the FCRA requirements for CRAs. Upon request from the Client, RPS may provide a consumer report (reports), as defined by §603(d) of the FCRA, rental screening scores, statistical summary reports, and any other services specifically agreed in writing by the Client and RPS. RPS makes no representations or warranties regarding the credit-worthiness of or suitability for residency of any individual. RPS will perform its obligations pursuant to the signed Screening Services Agreement (Agreement) as an independent contractor.

B. RPS CLIENT ROLE

Client will order reports as an end user and shall not disclose, disseminate, share, sublicense, resell or otherwise redistribute reports to any parent, subsidiary, affiliate or other third party. Client will perform its obligations pursuant to the signed Agreement as an independent contractor.

C. RPS CLIENT RESPONSIBILITIES

Client understands and acknowledges its obligations under, and shall at all times abide by all applicable federal, state, and local laws and regulations of governing consumer's right to privacy, including without limitation any applicable non-solicitation laws and regulations, the FCRA, state consumer reporting laws, and the Gramm-Leach-Bliley Act (GLB) in ordering and using reports.

- System and Account Set-Up – While RPS may provide assistance with system set-up, it is the responsibility of the Client to ensure all settings, including score thresholds, meet their business needs and comply with all laws and regulations.
- Approval Decisions – While RPS provides Clients tools to assist in the applicant decisioning process, Client acknowledges that it makes, and is responsible for, any decision to accept or reject an applicant. It is the responsibility of the Client, working with their legal counsel, to ensure that their applicant approval process complies with all laws and regulations.
- Permissible Purpose - Client will only order and use reports solely for the permissible purpose established in the signed Screening Services Agreement.
- Consumer Authorization – Client will only order and use reports after obtaining written consumer authorization, with verifying government issued identification of consumer.
- Retention of Documents – All written consumer authorizations, along with all adverse action letters provided to consumers, including copies of government issued identification needed to verify the identity of the applicant must be retained by the Client for no less than five (5) years and must be made available to RPS, in a timely manner, if requested.
- Verification of Data – Client shall conduct an independent verification of the information contained in the report to ensure that it pertains to the applicant before taking any adverse action.
- Adverse Action – Whenever Client takes adverse action against a consumer that is based in whole or in part on information contained in a report obtained from RPS, Client shall provide such consumer with an adverse action letter as required by FCRA §615(a). As required by the FCRA §615(a)(3)(A), the adverse action letter must include contact information for RPS as furnisher of the report. Also required by the FCRA §615(a)(3)(B), the adverse action letter must include a statement that RPS did not make the decision to take the adverse action and is unable to provide the consumer the specific reasons why the adverse action was taken. Therefore, Client shall not direct consumers to RPS to find out why the consumer was declined, as RPS cannot advise a consumer about why the consumer was declined.
- Referral to RPS – Client shall refer consumers who wish to obtain a copy of their file, or who wish to dispute an item on their file, to RPS at either its address or the toll-free number for consumer assistance.

II. On-Going Duties

A. COMPLIANCE WITH APPLICABLE LAW

Client has certain on-going duties including, as an example but without limitation, Client's duties when adverse action is taken by Client with respect to a Consumer's application and Consumer re-investigations. Client will at all times be compliant with such on-going duties. Some of these duties are described in the following FCRA Appendices, and there may be similar and/or additional state or local legal or regulatory requirements imposed on an "End-User" of Consumer Reports:

- Prescribed Notice to User Responsibilities (Appendix N to Part 1022 of Title 12 Code of Federal Regulations).
- Prescribed Summary of Consumer Rights (Appendix K to Part 1022 of Title 12 Code of Federal Regulations).
- Prescribed Notice of Furnisher Responsibility (Appendix M to Part 1022 of Title 12 Code of Federal Regulations).
- Prescribed Summary of Identity Theft Rights (Appendix I to Part 1022 of Title 12 Code of Federal Regulations).

It is Client's duty to maintain updated copies and comply with the requirements set forth in such Appendices and all Applicable Law. Copies of the above referenced FCRA Appendices were remitted to Client on or about the Effective Date of the Agreement, and the full text of the FCRA and the above-referenced Appendices can be obtained from the Consumer Financial Protection Bureau website at www.consumerfinance.gov (as such web site address may be changed from time to time).

Changes in Applicable Law or RPS's Policies and Procedures may require modifications to the Compliance Requirements from time to time, and Client shall comply with said modifications and will provide such other representations, warranties, or compliance materials as shall be required by RPS. Client agrees to only use faxes in secure office locations and to comply with requests to certify authorized/secured fax numbers on a requested basis.

B. CONSUMER IDENTIFIERS

RPS relies on the accuracy of the inquiry information Client provides in its screening request, which is very important in matching potential records to Consumers. To request a Consumer Report, Client shall complete all system required fields and **at a minimum** provide the following information regarding the Consumer:

1. Full first, middle and last name;
2. Date of birth, including month, day, and year;
3. Current address; and
4. Social Security Number or Tax Identification Number.

Additional identifiers may be required, based on the product offering.

C. NOTIFICATION OF CHANGES

Client has a duty to notify RPS in the event of a relocation of business, a change in the authorized officer signing the agreement, a change in the nature of Client's business.

III. System Access and Security Requirements

The following information security controls are required to reduce unauthorized access to consumer information. It is Client's responsibility to implement these controls. RPS reserves the right to make changes to these Access Security Requirements without prior notification. The information provided herewith provides minimum baselines for information security. In requesting Consumer Reports from RPS, Client agrees to follow these requirements. These requirements are applicable to all systems and devices used to access, transmit, process, or store consumer reports provided by RPS, including all information contained within the consumer report, or other information provided by RPS ("RPS data"):

A. IMPLEMENT STRONG ACCESS CONTROL MEASURES

1.1 All credentials such as User names/identifiers/account numbers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party.

1.2 If using third party or proprietary system to access RPS's systems, ensure that the access must be preceded by authenticating users to the application and/or system (e.g. application based authentication, Active Directory, etc.) utilized for accessing RPS data/systems.

1.3 If the third party or third party software or proprietary system or software, used to access RPS's data/systems, is replaced or no longer in use, the passwords should be changed immediately.

1.4 Create a unique user ID for each user to enable individual authentication and accountability for access to RPS's infrastructure. Each user of the system access software must also have a unique logon password.

1.5 User IDs and passwords shall only be assigned to authorized individuals based on least privilege necessary to perform job responsibilities.

1.6 User IDs and passwords must not be shared, posted, or otherwise divulged in any manner.

1.7 Develop strong passwords that are:

- Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
- Contain a minimum of eight (8) alphabetic and numeric characters for standard user accounts
- For interactive sessions (i.e. non system-to-system) ensure that passwords/passwords are changed periodically (every 90 days is recommended)

1.8 Passwords (e.g. user/account password) must be changed immediately when:

- Any system access software is replaced by another system access software or is no longer used
- The hardware on which the software resides is upgraded, changed or disposed
- Any suspicion of password being disclosed to an unauthorized party (see section 4.3 for reporting requirements)

1.9 Ensure that passwords are not transmitted, displayed or stored in clear text; protect all end user (e.g. internal and external) passwords using, for example, encryption or a cryptographic hashing algorithm also known as "one-way" encryption. When using encryption, ensure that strong encryption algorithms are utilized (e.g. AES 256 or above).

1.10 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations. Systems should be manually locked before being left unattended.

1.11 Active logins to credit information systems must be configured with a 30-minute inactive session timeout.

1.12 Ensure that personnel who are authorized access to credit information have a business need to access such information and understand these requirements to access such information are only for the permissible purposes listed in the Permissible Purpose Information section of the membership application.

1.13 Client must NOT install Peer-to-Peer file sharing software on systems used to access, transmit or store RPS data.

1.14 Ensure that Client employees do not access their own credit reports or those reports of any family member(s) or friend(s) unless it is in connection with a credit transaction or for another permissible purpose.

1.15 Implement a process to terminate access rights immediately for users who access RPS credit information when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.

1.16 Implement a process to perform periodic user account reviews to validate whether access is needed as well as the privileges assigned.

1.17 Implement a process to periodically review user activities and account usage, ensure the user activities are consistent with the individual job responsibility, business need, and in line with contractual obligations.

1.18 Implement physical security controls to prevent unauthorized entry to Client's facility and access to systems used to obtain credit information. Ensure that access is controlled with badge readers, other systems, or devices including authorized lock and key.

B. MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

2.1 Keep operating system(s), firewalls, routers, servers, personal computers (laptops and desktops) and all other systems current with appropriate system patches and updates.

2.2 Configure infrastructure such as firewalls, routers, servers, tablets, smart phones, personal computers (laptops and desktops), and similar components to industry best security practices, including disabling unnecessary services or features, and removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.

2.3 Implement and follow current best security practices for computer virus detection scanning services and procedures:

- Use, implement and maintain a current, commercially available anti-virus software on all systems, if applicable anti-virus technology exists. Anti-virus software deployed must be capable to detect, remove, and protect against all known types malicious software such as viruses, worms, spyware, adware, Trojans, and root-kits.
- Ensure that all anti-virus software is current, actively running, and generating audit logs; ensure that anti-virus software is enabled for automatic updates and performs scans on a regular basis.
- If you suspect an actual or potential virus infecting a system, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

C. PROTECT DATA

3.1 Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).

3.2 RPS data is classified Confidential and must be secured to in accordance with the requirements mentioned in this document at a minimum.

3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.

3.4 Encrypt all RPS data and information when stored electronically on any system including but not limited to laptops, tablets, personal computers, servers, databases using strong encryption such AES 256 or above.

3.5 RPS data must not be stored locally on smart tablets and smart phones such as iPads, iPhones, Android based devices, etc.

3.6 When using smart tablets or smart phones to access RPS data, ensure that such devices are protected via device pass-code.

3.7 Applications utilized to access RPS data via smart tablets or smart phones must protect data while in transmission such as SSL protection and/or use of VPN, etc.

3.8 Only open email attachments and links from trusted sources and after verifying legitimacy.

3.9 When no longer in use, ensure that hard-copy materials containing RPS data are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.

3.10 When no longer in use, electronic media containing RPS data is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).

D. MAINTAIN AN INFORMATION SECURITY POLICY

4.1 Develop and follow a security plan to protect the confidentiality and integrity of personal consumer information as required under the GLB Safeguards Rule.

4.2 Suitable to complexity and size of the organization, establish and publish information security and acceptable user policies identifying user responsibilities and addressing requirements in line with this document and applicable laws and regulations.

4.3 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators. *If you believe RPS data may have been compromised, immediately notify RPS within twenty-four (24) hours or per agreed contractual notification timeline.*

4.4 The FACTA Disposal Rules requires that Client implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.

4.5 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security in the organization.

4.6 When using third party service providers (e.g. application service providers) to access, transmit, store or process RPS data, ensure that service provider is compliant with RPS's requirements stated herein and has been approved by RPS. If the service provider is in the process of becoming compliant, it is Client's responsibility to ensure the service provider is engaged with RPS and an exception is granted in writing.

E. BUILD AND MAINTAIN A SECURE NETWORK

5.1 Protect Internet connections with dedicated, industry-recognized firewalls that are configured and managed using industry best security practices.

5.2 Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.

5.3 Administrative access to firewalls and servers must be performed through a secure internal wired connection only.

5.4 Any stand-alone computers that directly access the Internet must have a desktop firewall deployed that is installed and configured to block unnecessary/unused ports, services, and network traffic.

5.5 Change vendor defaults including but not limited to passwords, encryption keys, SNMP strings, and any other vendor defaults.

5.6 For wireless networks connected to or used for accessing or transmission of RPS data, ensure that networks are configured and firmware on wireless devices updated to support strong encryption (for example, IEEE 802.11i) for authentication and transmission over wireless networks.

5.7 When using service providers (e.g. software providers) to access RPS systems, access to third party tools/services must require multi-factor authentication.

F. REGULARLY MONITOR AND TEST NETWORKS

6.1 Perform regular tests on information systems (port scanning, virus scanning, internal/external vulnerability scanning). Ensure that issues identified via testing are remediated according to the issue severity (e.g. fix critical issues immediately, high severity in 15 days, etc.)

6.2 Ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit RPS data; establish a process for linking all access to such systems and applications. Ensure that security policies and procedures are in place to review security logs on daily or weekly basis and that follow-up to exceptions is required.

6.3 Use current best practices to protect telecommunications systems and any computer system or network device(s) used to provide Services hereunder to access RPS systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:

- protecting against intrusions;
- securing the computer systems and network devices;
- and protecting against intrusions of operating systems or software.

G. MOBILE AND CLOUD TECHNOLOGY

7.1 Storing RPS data on mobile devices is prohibited. Any exceptions must be obtained from RPS in writing; additional security requirements will apply.

7.2 Mobile applications development must follow industry known secure software development standard practices such as OWASP and OWASP Mobile Security Project adhering to common controls and addressing top risks.

7.3 Mobile applications development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.

7.4 When using cloud providers to access, transmit, store, or process RPS data ensure that:

- Appropriate due diligence is conducted to maintain compliance with applicable laws and regulations and contractual obligations

H. GENERAL

8.1 RPS may from time to time audit the security mechanisms Client maintains to safeguard access to RPS information, systems and electronic communications. Audits may include examination of systems security and associated administrative practices

8.2 In cases where the Client is accessing RPS information and systems via third party software, the Client agrees to make available to RPS upon request, audit trail information and management reports generated by the vendor software, regarding Client individual authorized users.

8.3 Client shall report actual security violations or incidents that impact RPS to RPS within twenty-four (24) hours or per agreed contractual notification timeline, as further provided in the Agreement. Client agrees to provide notice to RPS of any confirmed security breach that may involve data related to the contractual relationship, to the extent required under and in compliance with applicable law.

8.4 Client acknowledges and agrees that the Client (a) has received a copy of these requirements, (b) has read and understands Client's obligations described in the requirements, (c) will communicate the contents of the applicable requirements contained herein, and any subsequent updates hereto, to all employees that shall have access to RPS services, systems or data, and (d) will abide by the provisions of these requirements when accessing RPS data.

8.5 Client acknowledges and agrees that it is responsible for all activities of its employees/authorized users, and for assuring that mechanisms to access RPS services or data are secure and in compliance with its membership agreement.