PLEASE READ THESE INSTRUCTIONS CAREFULLY
BEFORE YOU BEGIN THE APPLICATION

An approved membership with Innovative Credit Solutions will give you access to order national criminal background reports. Please fill out the application (pages 2 - 6) completely. Return the application pages by e-mail to info@icscredit.com or fax to 888-571-7222. Please include a copy of your business license with the application.

- All pages must be signed and completed (no exceptions). Please make sure the credit card information is correct.
- Enter the information electronically on page 2 (the form will automatically fill the remaining pages) or a hand-written copy is acceptable.

- If there is a different billing contact and address, please provide this information.
- We must have a copy of your business license or a copy of the document that your state requires to operate a business.
- A copy of the current white or yellow pages ad for your business may be sufficient.
- We will need a telephone number and contact person that can be reached during the day. An e-mail address and fax number is also needed.
- If you have any questions, please call us at 800-345-2746 or e-mail your questions to info@icscredit.com. We also offer credit reports and driver record checks to assist you in making a well-informed decision.

INNOVATIVE CREDIT SOLUTIONS, INC.

Phone: 1-800-345-2746
Fax: 1-888-571-7222
info@icscredit.com

P O Box 1440
Lexington, SC 29071
www.icscredit.com

APPLICATION FOR SERVICE

COMPLETE ALL INFORMATION AND SIGN APPLICATION
INCLUDE COPY OF BUSINESS LICENSE WITH APPLICATION

BUSINESS INFORMATION

Name of Firm:				Federal Tax ID#	
Other business name(s) or dba:				Web Address:	
Phone:	Fax:		E-mail:		
Physical Address (No PO Box numbers)					
City:			State:	ZIP Code:	
Business Established:	Month	Year	How long at current address:	Years	Months
Does your business operate from a residence ☐ YES ☐ NO			Number of Employees:		
Contact Name:			Title:		
Phone:	Fax:		E-mail:		
Company name as listed with Directory Assistance:					
Nature of your Business (be specific):					
Services Offered/Products Sold:					
Permissible Purpose/Appropriate Use: ☐ Extending Credit ☐ Employment Purposes ☐ Tenant Screening ☐ Other Describe the specific purpose for which credit information will be used:					

BILLING INFORMATION

Billing Contact:	Phone:	E-mail:
Cost to Activate Account: $75.00 ☐ Option 1: $15.00 per Criminal Background Report ☐ Option 2: $7.50 per Criminal Background Report with $20.00 Monthly Minimum		
CREDIT CARD INFORMATION ☐ American Express ☐ Visa ☐ MasterCard ☐ Discover		
Credit Card #:	Exp Date	CVV # (digits on back of card)
Name on Card:		

Billing Address on Card:	City	State	Zip

Federal regulation requires that ICS, Inc. conduct an onsite property observation of your company. In most cases, this must be conducted prior to your account being established. Please note that ICS, Inc. contracts with a vendor to conduct these property observations and that vendor will be contacting you on behalf of ICS, Inc. to schedule an appointment. (The vendor usually contacts you within three days of receipt of application.)

SIGNATURE & AGREEMENT

I certify that I will use the Experian, Equifax, TransUnion background information for no other purpose other than what is stated in the Permissible Purpose/Appropriate Use section on this application and for the type of business listed on this application. **I will not resell the report to any third party**. I understand that if my system is used improperly by company personnel, or if my access codes are made available to any unauthorized personnel due to carelessness on the part of any employee of my company, I may be held responsible for financial losses, fees, or monetary charges that may be incurred and that my access privilege may be terminated. By signing below I authorize Innovative Credit Solutions, Inc. to charge the above listed credit card for all services provided. I certify that the above information is accurate. By signing, I warrant that I have the authority to sign on behalf of the company. I acknowledge that an onsite inspection will be required for new customers. A copy of the Company business license is included with this application.

Principal's Name (please print)	Title or Position:
Principal's Signature (required):	Date:

Disclaimer of Warranty: Because this service involves information provided from other sources, Innovative Credit Solutions, Inc. cannot and will not be an insurer or guarantor of the accuracy of reliability of the service of data released or stored. Innovative Credit Solutions does not guarantee or warrant the accuracy, timeliness, completeness, currentness, merchantability or fitness for a particular purpose of the service. Information in the service or the media on or through which the services are provided and shall not be liable to Subscriber or to any of the Subscribers customers for any loss or injury arising out of or caused in whole or part by Innovative Credit Solutions, Inc. acts or omissions, whether negligent or otherwise, in procuring, compiling, collecting, interpreting, reporting, communicating or delivering the services or information therein.

INNOVATIVE CREDIT SOLUTIONS, INC.
SUBSCRIBER AGREEMENT
For Criminal Report Purposes

This Agreement is made and entered into as of _____ ("Effective Date"), by and between Innovative Credit Solutions and (Company Name) _____

(Company Address) _____

1. End User is a (type of business) _____ and has a permissible purpose for obtaining criminal reports in accordance with the Fair Credit Reporting Act (15 U.S .C. § 1681 et seq.) including, without limitation, all amendments thereto ("FCRA"). The End User certifies its permissible purpose is:

   - In connection with the underwriting of insurance involving the consumer or review of existing policy holders for insurance underwriting purposes, or in connection with an insurance claim where written permission of the consumer has been obtained; or
   - In connection with a tenant screening application involving the consumer; or In accordance with the written instructions of the consumer; or
   - In connection with a employment screening application involving the potential or existing employee; or In accordance with the written instructions of the consumer; or
   - For a legitimate business need in connection with a business transaction that is initiated by the consumer; or
   - As a potential investor, servicer or current insurer in connection with a valuation of, or assessment of, the credit or prepayment risks.

2. End User certifies that End User shall use the criminal reports: (a) solely for the Subscriber's certified use(s); and (b) solely for End User's exclusive one-time use. End User shall not request, obtain or use criminal reports for any other purpose including, but not limited to, for the purpose of selling, leasing, renting or otherwise providing information obtained under this Agreement to any other party, whether alone, in conjunction with End User's own data, or otherwise in any service which is derived from the criminal reports. The criminal reports shall be requested by, and disclosed by End User only to End User's designated and authorized employees having a need to know and only to the extent necessary to enable End User to use the criminal reports in accordance with this Agreement. End User shall ensure that such designated and authorized employees shall not attempt to obtain any consumer reports on themselves, associates, or any other person except in the exercise of their official duties.
3. End User will maintain copies of all written authorizations for a minimum of five (5) years from the date of inquiry.
4. THE FCRA PROVIDES THAT ANY PERSON WHO KNOWINGLY AND WILLFULLY OBTAINS INFORMATION ON A CONSUMER FROM A CONSUMER REPORTING AGENCY UNDER FALSE PRETENSES SHALL BE FINED UNDER TITLE 18 OF THE UNITED STATES CODE OR IMPRISONED NOT MORE THAN TWO YEARS, OR BOTH.
5. End User shall use each criminal report only for a one-time use and shall hold the report in strict confidence, and not disclose it to any third parties; provided, however, that End User may, but is not required to, disclose the report to the subject of the report only in connection with an adverse action based on the report.
6. With just cause, such as violation of the terms of the End User's contract or a legal requirement, or a material change in existing legal requirements that adversely affects the End User's agreement, Reseller may, upon its election, discontinue serving the End User and cancel the agreement immediately.
7. End User will request criminal reports with the knowledge that the information is gathered from databases that are considered public and end users should not assume that information provided is current, complete or an accurate history of any individual. End users should review all federal, state and local laws before using this information during the process of intended transaction; hiring/ termination of employee, leasing, renting, selling or any other intention herein. Innovative Credit Solutions assumes no liability for any claims for damages arising from the use of this data beyond the actual cost of the searches performed.

End User:

Company Name: _____

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Innovative Credit Solutions

Signature: _____

Printed Name: _____

Title: _____

Date: _____

INNOVATIVE CREDIT SOLUTIONS, INC.

PHONE: 1-800-345-2746 FAX: 1-888-571-72222

END USER CERTIFICATION OF USE FOR EMPLOYMENT REPORTS

In compliance with the Federal Fair Credit Reporting Act as amended by the Consumer Credit Reporting Reform Act of 1996 (the "Act"), _____ ("End User") hereby certifies to Innovative Credit Solutions that it will comply with the following provisions:

1. End User will ensure that prior to procurement or causing the procurement of a consumer report for employment purposes:
    a. a clear and conspicuous disclosure has been made in writing to the consumer at any time before the report is procured or caused to be procured, in a document that consists solely of the disclosure, that a consumer report may be obtained for employment purposes; and
    b. the consumer has authorized in writing the procurement of the report by the End User.

2. In using a consumer report for employment purposes, before taking any adverse action based in whole or in part on the report, the End User shall provide to the consumer to whom the report relates
    a. a copy of the report; and
    b. a description in writing of the rights of the consumer under the Act, a copy of which is attached hereto ("Summary of Consumer Rights").

The information from the consumer report will not be used in violation of any applicable federal or state equal employment opportunity law or regulation.

End User hereby acknowledges receipt of the Summary of Consumer Rights.

_____

End User - Company Name

_____

Print Name

_____ _____

Signature Date

_____

Title

Access Security Requirements

The following information security controls are required to reduce unauthorized access to consumer information. It is your (company provided access to data through Innovative Credit Solutions, referred to as the "Company") responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to get an outside service provider to assist you. Innovative Credit Solutions 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 accessing Innovative Credit Solutions' services, Company agrees to follow these security requirements. These requirements are applicable to all systems and devices used to access, transmit, process, or store data:

1. Implement Strong Access Control Measures

1.1 All credentials such as Subscriber Code number, Subscriber Code passwords, User names/identifiers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party. No one from Innovative Credit Solutions will ever contact you and request your credentials.

1.2 If using third party or proprietary system to access Innovative Credit Solutions' 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 Innovative Credit Solutions data/systems.

1.3 If the third party or third party software or proprietary system or software, used to access Innovative Credit Solutions 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 Innovative Credit Solutions' 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. subscriber code passwords, user 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

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 algorithm 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 consumer information systems must be configured with a 30 minute inactive session timeout.

1.12 Ensure that personnel who are authorized access to consumer 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 Company must NOT install Peer-to-Peer file sharing software on systems used to access, transmit or store data.

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

1.15 Implement a process to terminate access rights immediately for users who access consumer information when those users are terminated or when they have a change in their job tasks and no longer require access to that 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 Company's facility and access to systems used to obtain consumer information. Ensure that access is controlled with badge readers, other systems, or devices including authorized lock and key.

2. 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.

3. 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 Consumer 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 Consumer 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 Consumer 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 Consumer data, ensure that such devices are protected via device pass-code.

3.7 Applications utilized to access Consumer 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 Consumer 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 Consumer 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).

Subscriber: _____
(please print)

Signature: _____

Print Name: _____

Date: _____

A Summary of Your Rights Under the Fair Credit Reporting Act

The federal Fair Credit Report Act (FCRA) is designed to promote accuracy, fairness, and privacy of information used in the process of granting credit. This information is supplied by public record sources, credit grantors and others to credit reporting agencies (CRA's) who organize and store that information for distribution to credit grantors, employers and insurers who are making credit, employment and insurance decisions about you. The FCRA gives suppliers and users of credit information, and CRA's specific responsibilities in connection with their respective roles in the credit granting and reporting process. The FCRA also gives you specific rights in dealing with these entities, as summarized below. You can find the complete text of the FCRA, 15 U.S.C. 1681 et seq., at the Federal Trade Commission's web site (http://www.ftc.gov). You may have additional rights under state law. You may contact a state or local consumer protection agency or a state attorney general to learn those rights.

- Access to your file is limited. Your file may only be accessed by those who have a permissible purpose recognized by the FCRA – usually to consider an application you have submitted to a creditor, insurer, employer, landlord, or other business, or to consider you for an unsolicited offer of credit.

- Your consent is required for reports that are provided to employers or that contain medical information. A CRA may not give a report about you to your employer, or prospective employers without your written consent. A CRA may not report medical information about you to creditors, insurers, or employers without your permission.

- You can find out what is in your file. Upon your request a CRA must give you all the information in your file, and a list of everyone who has requested it recently. However, you are not entitled to any information concerning "risk scores," "credit scores," or other economic predictors that are in your file. There is no charge for the report if a third party used the information in your file to take unfavorable action toward you and you request the report with 60 days of receiving notice that the information in your file was used by a third party unfavorably. You are also entitled to one free report every twelve months upon request if you certify that (1) you are unemployed and plan to seek employment within 60 days, (2) you are on welfare, or (3) your report is inaccurate due to fraud. Otherwise, a CRA may charge you a fee of up to eight dollars.

- You must be told if information in your file was a factor considered by a third party who took unfavorable actions toward you. Upon your request, anyone who considers information from a CRA and who takes unfavorable actions toward you—such as denying an application for credit, insurance, or employment—must give you the name, address, and phone number of the CRA that provided the information. Keep in mind that the third party, not the CRA, took the unfavorable action toward you and that the CRA will not be able to provide you with the reason for the unfavorable action.

- You can dispute inaccurate information with the CRA. If you tell a CRA that your file contains inaccurate information, the CRA must reinvestigate the items (usually within30 days) by presenting to its information source all relevant evidence you submit, unless your dispute is frivolous. The source must review your evidence and report its findings to the CRA. (The source also must advise national CRA's—to which it has provided data—of any error.) The CRA must give you a written report of the investigation, and a copy of your report if the investigation results in any change. If the CRA's investigation does not resolve the dispute, you may add a brief statement to your file. The CRA must normally include a summary of your dispute statement in future reports. If an item is deleted or a dispute statement is filed, you may ask that anyone who has recently received your report be notified of the change.

- Inaccurate information must be corrected or deleted. A CRA must remove inaccurate information from its files, usually within 30 days after you dispute it. However, the CRA is not required to remove accurate date from your file unless it is outdated (as described below) or cannot be verified. If your dispute results in any change to your report, the CRA cannot reinsert into your file a disputed item unless the information source verifies its accuracy and completeness. In addition, the CRA must give you a written notice telling you it has reinserted the

item. The notice must include the name, address and phone number of the information source.

- You can dispute inaccurate items with the source of the information. If you tell the third party who furnished information to a CRA—such as a creditor who reports to a CRA—that you dispute an item, it may not then report the information to a CRA without including a notice of your dispute. In addition, once you've notified the source of the error in writing, it may not continue to report the information if it is in fact an error.

- Outdated information may not be reported. In most cases, a CRA may not report negative information that is more than seven years old (ten years for bankruptcies).

- You may choose to exclude your name from CRA lists for unsolicited credit and insurance offers. Creditors and insurers may use file information as the basis for sending you unsolicited offers of credit or insurance. Such offers must include a toll-free telephone number for you to call and tell the CRA if you want your name and address removed from future lists or offers. If you notify the CRA through the toll-free number, if must keep you off the lists for two years. If you request, complete and return the CRA form provided for this purpose, you can have your name and address removed indefinitely.

- You may seek damages from violators. If a CRA, a user or (in some cases) a provider of CRA data, violates the FCRA, you may sue them in state or federal court.

The FCRA gives several different federal agencies authority to enforce the FCRA:

CRA's, creditors and others not listed below	Federal Trade Commission Bureau of Consumer Protection – FCRA Washington, DC 20580 ● 202-326-3761
National banks, federal branches/agencies of foreign banks (word "National" or initials "N.A." appear in or after bank's name	Office of the Comptroller of the Currency Compliance Management, Mail Stop 6-6 Washington, DC 20219 ● 202-452-3693
Federal Reserve System member banks (except national banks, and federal branches/agencies of foreign banks)	Federal Reserve Board Division of Consumer & Community Affairs Washington, DC 20551 ● 202-452-3693
Savings associations and federally chartered savings banks (word "Federal" or initials "F.S.B." appear in federal institution's name)	Office of Thrift Supervision Consumer Programs Washington, DC 205520 ● 800-842-6929
Federal credit unions (words "Federal Credit Union" appear in institution's name)	National Credit Union Administration 1775 Duke Street Alexandria, VA 22314 ● 703-518-6360
Banks that are state-chartered, or are not Federal Reserve System members	Federal Deposit insurance Corporation Division of Compliance & Consumer Affairs Washington, DC 20429 ● 800-934-FDIC
Air, surface, or rail common carriers regulated by former Civil Aeronautics Board or Interstate Commerce Commission	Department of Transportation Office of Financial Management Washington, DC 20590 ● 202-366-1306