The Landlord Association of Pennsylvania
1414 Millard Street ▪ Bethlehem, PA 18018
Tel. (610) 867-8940 ▪ Fax (610) 867-8604

MEMBERSHIP APPLICATION

Date of Application: _____

Important: ***All information must be completed in its entirety. Please print clearly and legibly to help ensure accurate and timely processing.***

A. GENERAL MEMBER INFORMATION

***New Membership requires a "Site Inspection"**

Member Name: _____ Years in Business: _____

Type of Ownership: Indicate one ❑ Partnership ❑ Sole Owner ❑ Nonprofit ❑ Corporation

Other business name(s) or dba: _____ EIN Number: _____

Hours: Indicate one ☐ 8 am – 5 pm ☐ 9am – 6 pm ☐ Other _____ Days: ☐ M ☐ T ☐ W ☐ TH ☐ F ☐ S ☐ S

Have you previously applied or have been a LAPA Member ❑ Yes ❑ No If Yes, when?

Under what name? _____

Physical Street Address (no P.O Box numbers please): _____

City: _____ State: _____ Zip: _____ How long: _____ Yrs _____ Mos.

Type of Property: Indicate one ❑ Residential ❑ Commercial Phone: ( ) Fax: ( )

B. PROPERTY OWNER:

I understand that the information provided below will be used to obtain a consumer credit report, and my credit worthiness may be considered when making a decision to grant membership.

Principal Name: _____

Title or Position: _____ Phone: ( )

Social Security Number: _____ Date of Birth: _____

Residential Street Address: _____

City: _____ State: _____ Zip: _____

C. LANDLORD PROOF/LICENSE CONFIRMATION:

(For security purposes, all new members are required to provide a minimum of THREE forms of ID for membership)

MUST HAVE	Pick 1 Additional Proof
❑ **Photo ID**	❑ **Copy of Landlord License**
❑ **Copies of 3 different signed Rental Applications**	❑ **Copy of Rental Property Title**
***If Property Management, include a list of all properties**	❑ **Copy of Rental Tax Bills**
	❑ **Copy of Rental Insurance Documents**

D. ADDITIONAL INFORMATION:

Type of business: _____ Do you need a purchase order? ❑ Yes ❑ NO PO# _____

Do you have an Investigation License? ❑ Yes ❑ No If yes, please provide a copy with this application.

How many Credit Reports will you be accessing monthly? _____

Do you qualify for tax exemptions? ❑ Yes ❑ No If yes, please provide proof.

Website: _____

E. PERMISSABLE PURPOSE INFORMATION: *(Application will not be processed unless this information is provided below)*
Describe the specific purpose for which LAPA credit information will be used:

To check and verify credit history for the purpose of screening prospective tenants

F. BILLING ADDRESS:

Contact Name: _____ Phone: _____
Address: _____
City: _____ State: _____ Zip: _____
County: _____

G. BANKING REFERENCES: *(Please provide the name of the bank which maintains your business checking account)*

Bank: _____ Phone: _____
Address: _____
City: _____ State: _____ Zip: _____
Business Checking Account: _____

I have read and understand the "**FCRA** and **GLB** Requirements" notice and **LAPA'S** "Access Security Requirements" and will take all reasonable measures to enforce them within my facility. I certify that I will use the **LAPA** credit report for no other purpose other than what is stated in the Permissible Purpose section on this application. I will not resell the report to any consumer directly or indirectly. 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 privileges may be terminated.

Member acknowledges that he/she has received and read a copy of the current Terms and Conditions of Membership for **LAPA. LAPA** reserves the right at anytime without notice, to amend the Terms and Conditions of Membership.
MEMBER ACKNOWLEDGES AND ACCEPTS FULL RESPONSIBILITY AND GUARANTEES PAYMENT FOR ALL SERVICES RENDERED THROUGH **LAPA.**

Initial: _____

Member must notify LAPA immediately by telephone or writing if their internet passwords are lost or stolen. Member is responsible for all reports ordered under their company password. Failure to notify LAPA of the loss of your passwords may result in the posting of significant charges to the credit card account you identify on your application.

Initial:_____

Member agrees that LAPA may pursue all avenues of collection, including use of collection agencies, and authorizes LAPA to prepare and submit credit card charges using any/or all cards listed above to recover all charges and all unpaid accounts due.

Initial: _____

Important Tax Notice

Credit Reports are subject to sales tax for members located in the state of Pennsylvania. If you are located in PA and are tax exempt for any reason, please submit a statement of your tax exemption certificate along with this application. If you remit a use tax directly to the state, please submit a statement of use tax or a letter on your letterhead which states that you pay use tax.

All replications of the Membership Application shall be deemed an original.

I certify that I have read the above statements and all information provided is accurate and hereby authorize the Bank & Business References to release information to LAPA.

_____
Member Name

_____
Type or Print Name and Title of Owner or Officer

_____ _____
Authorized Signature Date

LANDLORD ASSOCIATION OF PENNSYLVANIA
(LAPA)
SUBSCRIBER SERVICE AGREEMENT

Subscriber Service Agreement entered into as of _____ by **Landlord Association**
(Date)

of Pennsylvania (LAPA) and _____
("Subscriber")

SECTION ONE. Statement of **LAPA** and Subscriber Responsibilities:

LAPA Agrees:

1.1 **LAPA** shall resell to Subscriber on request, credit information on consumers, businesses or corporations stored in **LAPA** computerized credit reporting system or obtained from other reliable sources available to same.

1.2 **LAPA** will exercise it best efforts to deliver credit or other information requested by Subscriber in an expeditious and efficient manner, but it shall have no obligation or liability to Subscriber for the accuracy, timeliness, completeness, merchantability or fitness for a particular purpose of the services, information in the services or the media on or through which the services are provided under this agreement.

1.3 **LAPA** shall respectively exercise its best efforts to furnish to Subscriber accurate and reliable information, but does not guarantee the correctness, currency or completeness of such information. Neither **LAPA**, nor its officers, employees, agents or suppliers shall be liable to Subscriber for any claim, injury or damage consequent upon furnishing such information.

Subscriber Agrees:

1.4 Subscriber shall provide **LAPA** with appropriate identifying information as to itself and the consumer when requesting information.

1.5 Subscriber hereby certifies and agrees that its operation is in compliance with Public Law 91-508 (Fair Credit Reporting Act) and all other applicable state and federal statutes and will request and use credit information received from **LAPA** solely in connection with transactions pursuant to the following terms:

1.6 Subscriber agrees to pay **LAPA** the applicable charge quoted by **LAPA** to Subscriber for the various services rendered to Subscriber. Payment by Subscriber shall be due twenty (20) days following receipt of invoice. A late payment charge of 1½% per month will be imposed on overdue payments. Subscriber will be liable for all legal and other costs and expenses incurred by **Subscriber**, including but not limited to reasonable attorneys' fees in the event that **LAPA** must take action to secure payment for services rendered to Subscriber.

1.7 Subscriber hereby certifies and agrees that the use of **LAPA** credit reports will not be used for any other purpose other than what is stated in the Permissible Purpose section on this agreement and for the type of business listed on this agreement.

1.8 Subscriber hereby certifies and agrees to not resell the report to any consumer directly or indirectly.

1.9 Subscriber hereby certifies and agrees that it is responsible for the security of its Subscriber number and password assigned to this account and all usage resulting therefrom. Subscriber acknowledges that the services it receives from **LAPA** under this agreement include personal information on individual consumers and, as such, require confidential treatment.

1.10 Acknowledge that many services containing Experian information also contain information from the Death Master File as issued by the Social Security Administration ("DMF"); certify pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 C.F.R. § 1110.102 that, consistent with its applicable FCRA or GLB use of Experian information, the use of deceased flags or other indicia within the Experian information is restricted to legitimate fraud prevention or business purposes in compliance with applicable laws, rules regulations, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. § 1110.102(a)(1); and certify that you will not take any adverse action against any consumer without further investigation to verify the information from the deceased flags or other indicia within the Experian information.

1.11 Certify that you shall implement and maintain a comprehensive information security program written in one or more readily accessible parts and that contains administrative, technical, and physical safeguards that are appropriate to the subscriber's size and complexity, the nature and scope of its activities, and the sensitivity of the information provided to the subscriber; and that such safeguards shall include the elements set forth in 16 C.F.R. § 314.4 and shall be reasonably designed to (i) insure the security and confidentiality of the information provided by Reseller, (ii) protect against any anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer.

SECTION TWO Requests for Employment Reports:

Subscriber Agrees:

2.1 Subscriber will provide a clear and conspicuous disclosure (in a document that consists solely of the disclosure) to the consumer indicating that a consumer report may be obtained for the purpose of employment and it will receive, in writing, the consumer's consent to procure a consumer report.

2.2 Subscriber will adhere to all applicable federal or state equal employment opportunity laws or regulations with respect to information received from the consumer report.

2.3 Before taking any adverse action based on information obtained from the consumer report, Subscriber agrees to provide the consumer with a copy of the report and a written description of the consumer's rights under the provisions of the Federal Trade Commission Section 609(c)(3).

SECTION THREE. Covenants and Indemnification:

3.1 **LAPA** shall indemnify, defend and hold Subscriber harmless from and against any and all costs and liabilities which may be asserted against Subscriber based upon improper use by **LAPA** of credit or other information furnished to **LAPA** by Subscriber. Subscriber shall indemnify, defend and hold **LAPA** harmless from and against any and all costs and liabilities which may be asserted against **LAPA** based upon the improper use by Subscriber of credit or other information furnished to Subscriber by **LAPA**.

3.2 This agreement shall continue in force without any fixed date of termination, but either **LAPA** or Subscriber may terminate the Agreement upon thirty days (30) prior notice to the other.

3.3 **LAPA** shall have no obligation or liability for or on the account of any mechanical or other breakdown, malfunction, or defect in computer or facilities or computer programs utilized by **LAPA** or Experian or any delay or failure in **LAPA's** performance under this Agreement when such is beyond the reasonable control of **LAPA**. **LAPA** will use reasonable efforts to prevent such delay or failure and shall attempt to correct any such delay or failure as promptly as possible.

3.4 The warranties set forth in this Agreement apply to the performance of both parties hereunder, and are in lieu of all other warranties, expressed or implied, including without limitation, the warranties of merchantability and fitness for a particular purpose which are hereby disclaimed.

Subscriber's type of business: _____

Purpose for which the reports will be used: To check and verify credit history for the purpose of screening prospective tenants

In Witness Whereof. **LAPA** and Subscriber have caused this Agreement to be executed by their duly authorized representatives as of the date first above written.

Member Name: _____

Member Address: _____

_____

Contact Name: _____ Email Address: _____

Phone Number: _____ Fax Number: _____

By: _____ _____

(Authorized Signature) *(Print Name and Title)*

The Landlord Association of Pennsylvania
1414 Millard Street ▪ Bethlehem, Pa 18018
Tel. (610) 867-8940 ▪ Fax (610) 867-8604

PERSONAL GUARANTEE AGREEMENT

I certify that I am the person named below. As principal of _____
(Member Name)

I authorize LAPA to review my credit profile report to be used in conjunction with this application for membership and guarantee payment of any and all credit-reporting obligations to the member listed above.

Name: _____ Social Security #: _____

Home Address: _____

_____

Previous Address: _____

_____

_____

_____
Signature and Title

The Landlord Association of Pennsylvania

FCRA and GLB Requirements

Federal Fair Credit Reporting Act (as amended by the
Consumer Credit Reporting Reform Act of 1996)

Although the FCRA primarily regulates the operations of consumer credit reporting agencies, it also affects you as a user of information. We suggest that you and your employees become familiar with the following sections in particular:

- § 604. Permissible Purposes of Reports
- § 607. Compliance Procedures
- § 615. Requirement on users of consumer reports
- § 616. Civil liability for willful noncompliance
- § 617. Civil liability for negligent noncompliance
- § 619. Obtaining information under false pretenses
- § 621. Administrative Enforcement
- § 623. Responsibilities of Furnishers of Information to Consumer Reporting Agencies
- § 628. Disposal of Records

Each of these sections is of direct consequence to users who obtain reports on consumers.

In addition to the above, please read and understand your obligations and responsibilities under the FCRA and GLB.

As directed by the law, credit reports may be issued only if they are to be used for extending credit, review or collection of an account, employment purposes, underwriting insurance or in connection with some other legitimate business transaction such as in investment, partnership, etc. It is imperative that you identify each request for a report to be used for employment purposes when such report is ordered. Additional state laws may also impact your usage of reports for employment purposes.

We strongly endorse the letter and spirit of the Federal Fair Credit Reporting Act. We believe that this law and similar state laws recognize and preserve the delicate balance between the rights of the consumer and the legitimate needs of commerce.

In addition to the Federal Fair Credit Reporting Act, other federal and state laws addressing such topics as computer crime and unauthorized access to protected databases have also been enacted. As a prospective user of consumer reports, we expect that you and your staff will comply with all relevant federal statutes and the statutes and regulations of the states in which you operate.

We support consumer reporting legislation that will assure fair and
equitable treatment for all consumers and users of credit information.

_____ _____

Signature/Title Date

GLB SAFEGUARDS

_____ (Subscriber) certifies to CBA Lehigh Valley and Landlord Association of Pennsylvania that Subscriber has determined that its use of the Identity Verification portion of the Social Security Number Search is solely **for the purpose of protecting against or preventing actual or potential fraud, unauthorized transactions, claims or other liability** pursuant to the exception under Section 6802(e)(3)(B) of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 *et seq*. (GLBA), and for no other purpose. Subscriber shall comply with all requirements set forth in the GLBA and shall implement and maintain a comprehensive information security program written in one or more readily accessible parts and that contains administrative, technical, and physical safeguards that are appropriate to Subscriber's size and complexity, the nature and scope of its activities, and the sensitivity of the information provided to Subscriber by CBALV and LAPA. Such safeguards shall include the elements set forth in 16 C.F.R. § 314.4 and shall be reasonably designed to (i) insure the security and confidentiality of the information provided by CBA Lehigh Valley, (ii) protect against any anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer.

Subscriber shall read and understand all responsibilities under the GLB Act.

Subscriber agrees to limit use for the appropriate use and appropriate industry as listed below.

☐ Subscriber represents that (1) the person signing this Acknowledgment has all right, power and authority to sign this Acknowledgment on behalf of Subscriber; (2) Subscriber has full power and authority and all necessary authorizations to comply with the terms of this Acknowledgment and to perform its obligations hereunder; and (3) by signing this Acknowledgment with an electronic signature, Subscriber (a) shall comply with all applicable electronic records and signatures laws, including but not limited to the Electronic Signatures in Global and National Commerce Act; and (b) hereby acknowledges that its electronic signature is effective and will not dispute the legally binding nature, validity or enforceability of this Acknowledgment based on the fact that the terms were accepted with an electronic signature.

Type of Business: Tenant Screening
(example: utility provider, tenant screening, employment screening, collection, Government, etc)

Appropriate Use: Fraud
(choose one: pre-employment screening, collections, fraud prevention)

_____ _____
Signature Date

_____
Print Name

_____
Title

CREDIT SCORING SERVICES AGREEMENT

This Credit Scoring Services Agreement, ("Agreement"), dated: _____ ____, between _____ ("End User") and Landlord Association of Pennsylvania ("Provider")

WHEREAS, Provider is an authorized reseller of Experian Information Solutions, Inc. ("Experian"); and

WHEREAS, Experian and Fair, Isaac Corporation ("Fair, Isaac") offer the "Experian/Fair, Isaac Model", consisting of the application of a risk model developed by Experian and Fair, Isaac which employs a proprietary algorithm and which, when applied to credit information relating to individuals with whom the End User contemplates entering into a credit relationship will result in a numerical score (the "Score" and collectively, "Scores"); the purpose of the models being to rank said individuals in order of the risk of unsatisfactory payment.

NOW, THEREFORE, For good and valuable consideration and intending to be legally bound, End User and Provider hereby agree as follows:

1. General Provisions

A. Subject of Agreement. The subject of this Agreement is End User's purchase of Scores produced from the Experian/Fair, Isaac Model from Provider.

B. Application. This Agreement applies to all uses of the Experian/Fair, Isaac Model by End User during the term of this agreement.

C. Term. The term of this agreement runs concurrent with active membership.

2. Experian/Fair, Isaac Scores

A. Generally. Upon request by End User during the Term, Provider will provide End User with the Scores.

B. Time of Performance. Provider will use commercially reasonable efforts to provide the Experian/Fair Isaac Model as expeditiously as possible and in a timely manner; provided, however, Provider will have no liability to End User hereunder for delays in providing such Experian/Fair, Isaac Model.

C. Warranty. Provider warrants that the Scores are empirically derived and statistically sound predictors of consumer credit risk on the data from which they were developed when applied to the population for which they were developed. Provider further warrants that so long as it provides the Scores, the Scores will not contain or use any prohibited basis as defined by the federal Equal Credit Opportunity Act, 15 USC Section 1691 *et seq*. or Regulation B promulgated thereunder. THE FOREGOING WARRANTIES ARE THE ONLY WARRANTIES PROVIDER HAS GIVEN END USER WITH RESPECT TO THE SCORES, AND SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, PROVIDER MIGHT HAVE GIVEN END USER WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. End User's rights under the foregoing warranties are expressly conditioned upon End User's periodic revalidation of the Experian/Fair, Isaac Model in compliance with the requirements of Regulation B as it may be amended from time to time (12 CFR Section 202 *et seq*.).

D. Release. End User hereby releases and holds harmless Provider, Fair Isaac and/or Experian and their respective officers, directors, employees, agents, sister or affiliated companies, and any third-party contractors or suppliers of Provider, Fair, Isaac or Experian from liability for any damages, losses, costs or expenses, whether direct or indirect, suffered or incurred by End User resulting from any failure of the Scores to accurately predict that a United States consumer will repay their existing or future credit obligations satisfactorily.

3. Fees - $1.00

4. Intellectual Property

A. No License. Nothing contained in this Agreement shall be deemed to grant End User any license, sublicense, copyright interest, proprietary rights, or other claim against or interest in any computer programs utilized by Provider, Experian and/or Fair, Isaac or any third party involved in the delivery of the scoring services hereunder. End User acknowledges that the Experian/Fair, Isaac Model and its associated intellectual property rights in its output are the property of Fair, Isaac.

B. End User Use Limitations. By providing the Scores to End User pursuant to this Agreement, Provider grants to End User a limited license to use information contained in reports generated by the Experian/Fair, Isaac Model solely in its own business with no right to sublicense or otherwise sell or distribute said information to third parties. Before directing Provider to deliver Scores to any third party (as may be permitted by this Agreement), End User agrees to enter into a contract with such third party that (1) limits use of the Scores by the third party only to the use permitted to the End User, and (2) identifies Experian and Fair, Isaac as express third party beneficiaries of such contract.

C. Proprietary Designations. End User shall not use, or permit its employees, agents and subcontractors to use, the trademarks, service marks, logos, names, or any other proprietary designations of Provider, Experian or Fair, Isaac

or their respective affiliates, whether registered or unregistered, without such party's prior written consent.

5. Compliance and Confidentiality

A. Compliance with Law. In performing this Agreement and in using information provided hereunder, End User will comply with all Federal, state, and local statutes, regulations, and rules applicable to consumer credit information and nondiscrimination in the extension of credit from time to time in effect during the Term. End User certifies that (1) it has a permissible purpose for obtaining the Scores in accordance with the federal Fair Credit Reporting Act, and any similar applicable state statute, (2) any use of the Scores for purposes of evaluating the credit risk associated with applicants, prospects or existing customers will be in a manner consistent with the provisions described in the Equal Credit Opportunity Act ("ECOA"), Regulation B, and/or the Fair Credit Reporting Act, and (3) the Scores will not be used for Adverse Action as defined by the Equal Credit Opportunity Act ("ECOA") or Regulation B, unless adverse action reason codes have been delivered to the End User along with the Scores.

B. Confidentiality. End User will maintain internal procedures to minimize the risk of unauthorized disclosure of information delivered hereunder. End User will take reasonable precautions to assure that such information will be held in strict confidence and disclosed only to those of its employees whose duties reasonably relate to the legitimate business purposes for which the information is requested or used and to no other person. Without limiting the generality of the foregoing, End User will take suitable precautions to prevent loss, compromise, or misuse of any tapes or other media containing consumer credit information while in the possession of End User and while in transport between the parties. End User certifies that it will not publicly disseminate any results of the validations or other reports derived from the Scores without each of Experian's and Fair, Isaac's express written permission.

C. Proprietary Criteria. Under no circumstances will End User attempt in any manner, directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by Experian and/or Fair, Isaac in performing the scoring services hereunder.

D. Consumer Disclosure. Notwithstanding any contrary provision of this Agreement, End User may disclose the Scores provided to End User under this Agreement (1) to credit applicants, when accompanied by the corresponding reason codes, in the context of bona fide lending transactions and decisions only, and (2) as clearly required by law.

6. Indemnification and Limitations

A. Indemnification of Provider, Experian and Fair, Isaac. End User will indemnify, defend, and hold each of Provider, Experian and Fair, Isaac harmless from and against any and all liabilities, damages, losses, claims, costs, and expenses (including attorneys' fees) arising out of or resulting from any nonperformance by End User of any obligations to be performed by End User under this Agreement, *provided that* Experian/Fair, Isaac have given End User prompt notice of, and the opportunity and the authority (but not the duty) to defend or settle any such claim.

B. Limitation of Liability. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, UNDER NO CIRCUMSTANCES WILL PROVIDER, EXPERIAN OR FAIR, ISAAC HAVE ANY OBLIGATION OR LIABILITY TO END USER FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES INCURRED BY END USER, REGARDLESS OF HOW SUCH DAMAGES ARISE AND OF WHETHER OR NOT END USER WAS ADVISED SUCH DAMAGES MIGHT ARISE. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF PROVIDER, EXPERIAN OR FAIR, ISAAC TO END USER EXCEED THE FEES PAID BY END USER PURSUANT TO THIS AGREEMENT DURING THE SIX MONTH PERIOD IMMEDIATELY PRECEDING THE DATE OF END USER'S CLAIM.

7. Miscellaneous

A. Third Parties. End User acknowledges that the Scores results from the joint efforts of Experian and Fair, Isaac. End User further acknowledges that each Experian and Fair, Isaac have a proprietary interest in said Scores and agrees that either Experian or the Fair, Isaac may enforce those rights as required.

B. Complete Agreement. This Agreement sets forth the entire understanding of End User and Provider with respect to the subject matter hereof and supersedes all prior letters of intent, agreements, covenants, arrangements, communications, representations, or warranties, whether oral or written, by any officer, employee, or representative of either party relating thereto.

IN WITNESS WHEREOF, End User has signed and delivered this Agreement.

By: _____ _____

(Authorized Signature) *(Title)*

_____ _____

(Print Name) *(Date)*

END USER AUTHORIZATION FORM (ONLINE ACCESS)

This form is to be used by Experian Reseller end user (End User) to identify the individual that will have access to Experian via the internet. The end user will submit all requests to create, change or lock End User access accounts and permissions to Experian systems and information via the Internet to the Experian Reseller Head Designate. End User(s) must be a duly appointed representative of the End User company and must be available to interact with Experian's Reseller on information and product access matters, in accordance with Experian Security Guidelines. Such Guidelines may be updated from time to time by Experian, and it is the responsibility of the End User to monitor the Guidelines for any updates. The Reseller End User Authorization Form must be signed by an authorized representative of the End User. End User acknowledges and agrees that they: 1) have received the Experian Security Guidelines, 2) have read and understands End User's obligations described in the Guidelines, 3) will communicate the contents of the Guidelines, and any subsequent updates thereto, to all employees that shall have access to Experian services via the Internet, and 4) will abide by the provisions of the Guidelines as well as the terms and conditions of the existing membership agreement(s). Changes in the End User status (e.g., transfer or termination) are to be reported to immediately to the Reseller Head Designate.

End User INFORMATION (All fields are required unless stated)

End User Status (Check One)	**Create**	☐	**Change**	☐	**Lock**	☐
User ID (first choice) [min. 6 chars.]						
User ID (second choice) [min. 6 chars.]						
User ID (third choice) [min. 6 chars.]						
Add Co ID (optional)						
End User Company Name (do not abbv.)						
Last Name						
First Name						
E-mail Address						
Telephone Number					Ext.	
Product(s) Requested	Hart Internet					
Comments						

REPRESENTATIVE INFORMATION (Signature Required)

As an End User of Experian's products and services over the Internet, I am acting as the authorized representative of the End User. I hereby submit the above individual as an End User of my company and authorize Experian's Reseller to direct all Information Security related questions to same.

Print Name		Title	
Signature		Date	

FOR RESELLER INTERNAL USE ONLY

(Do Not Write Below This Line)

Date Sent/Faxed to Reseller		Reseller Group Preamble	
Reseller Security Designate (Requestor)			
Signature		Date	

Access Security Requirements for
FCRA and GLB 5A Data

The following information security controls are required to reduce unauthorized access to consumer information. It is your (company provided access to Experian systems or data, 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. Experian 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 Experian's services, Company agrees to follow these security requirements. These requirements are applicable to all systems and devices used to access, transmit, process, or store Experian 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 Experian will ever contact you and request your credentials.

1.2 If using third party or proprietary system to access Experian'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 Experian data/systems.

1.3 If the third party or third party software or proprietary system or software, used to access Experian 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 Experian'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. 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 (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 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 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 Company must NOT install Peer-to-Peer file sharing software on systems used to access, transmit or store Experian data.

1.14 Ensure that Company 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 Experian 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 Company'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.

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

3.7 Applications utilized to access Experian 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 Experian 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 Experian 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).

4. 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 Experian data may have been compromised, immediately notify Experian within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).*

4.4 The FACTA Disposal Rules requires that Company 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 Experian data, ensure that service provider is compliant with Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian list of compliant service providers. If the service provider is in process of becoming compliant, it is Company responsibility to ensure the service provider is engaged with Experian and exception is granted in writing. *Approved certifications in lieu of EI3PA can be found in the Glossary section.*

5. 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 Experian 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 Experian systems, access to third party tools/services must require multi-factor authentication.

6. 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 Experian 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 Experian 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.

7. Mobile and Cloud Technology

7.1 Storing Experian data on mobile devices is prohibited. Any exceptions must be obtained from Experian 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 Mobility solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.

7.5 Mobile applications and data shall be hosted on devices through a secure container separate from any personal applications and data. See details below. Under no circumstances is Experian data to be exchanged between secured and non-secured applications on the mobile device.

7.6 In case of non-consumer access, that is, commercial/business-to-business (B2B) users accessing Experian data via mobile applications (internally developed or using a third party application), ensure that multi-factor authentication and/or adaptive/risk-based authentication mechanisms are utilized to authenticate users to application.

7.7 When using cloud providers to access, transmit, store, or process Experian data ensure that:

- Appropriate due diligence is conducted to maintain compliance with applicable laws and regulations and contractual obligations
- Cloud providers must have gone through independent audits and are compliant with one or more of the following standards, or a current equivalent as approved/recognized by Experian:
    - ISO 27001
    - PCI DSS
    - EI3PA
    - SSAE 16 – SOC 2 or SOC3
    - FISMA
    - CAI / CCM assessment

8. General

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

8.2 In cases where the Company is accessing Experian information and systems via third party software, the Company agrees to make available to Experian upon request, audit trail information and management reports generated by the vendor software, regarding Company individual Authorized Users.

8.3 Company shall be responsible for and ensure that third party software, which accesses Experian information systems, is secure, and protects this vendor software against unauthorized modification, copy and placement on systems which have not been authorized for its use.

8.4 Company shall conduct software development (for software which accesses Experian information systems; this applies to both in-house or outsourced software development) based on the following requirements:

8.4.1 Software development must follow industry known secure software development standard practices such as OWASP adhering to common controls and addressing top risks.

8.4.2 Software 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.

8.4.3 Software solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.

8.5 Reasonable access to audit trail reports of systems utilized to access Experian systems shall be made available to Experian upon request, for example during breach investigation or while performing audits

8.6 Data requests from Company to Experian must include the IP address of the device from which the request originated (i.e., the requesting client's IP address), where applicable.

8.7 Company shall report actual security violations or incidents that impact Experian to Experian within twenty-four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to Experian 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. Telephone notification is preferred at 800-295-4305, Email notification will be sent to regulatorycompliance@experian.com

8.8 Company acknowledges and agrees that the Company (a) has received a copy of these requirements, (b) has read and understands Company'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 Experian services, systems or data, and (d) will abide by the provisions of these requirements when accessing Experian data.

8.9 Company understands that its use of Experian networking and computing resources may be monitored and audited by Experian, without further notice.

8.10 Company acknowledges and agrees that it is responsible for all activities of its employees/Authorized users, and for assuring that mechanisms to access Experian services or data are secure and in compliance with its membership agreement.

8.11 When using third party service providers to access, transmit, or store Experian data, additional documentation may be required by Experian.

Record Retention: The Federal Equal Credit Opportunity Act states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the ECOA, Experian requires that you retain the credit application and, if applicable, a purchase agreement for a period of not less than 25 months. When conducting an investigation, particularly following a consumer complaint that your company impermissibly accessed their credit report, Experian will contact you and will request a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract.

"Under Section 621 (a) (2) (A) of the FCRA, any person that violates any of the provisions of the FCRA may be liable for a civil penalty of not more than $3,500 per violation."

Internet Delivery Security Requirements

In addition to the above, following requirements apply where Company and their employees or an authorized agent/s acting on behalf of the Company are provided access to Experian provided services via Internet ("Internet Access").

General requirements

1. The Company shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with Experian on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to Experian provided services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such functions.
2. The Company's Head Security Designate or Security Designate shall in turn review all employee requests for Internet access approval. The Head Security Designate or its Security Designate shall determine the appropriate access to each Experian product based upon the legitimate business needs of each employee. Experian shall reserve the right to terminate any accounts it deems a security threat to its systems and/or consumer data.
3. Unless automated means become available, the Company shall request employee's (Internet) user access via the Head Security Designate/Security Designate in writing, in the format approved by Experian. Those employees approved by the Head Security Designate or Security Designate for Internet access ("Authorized Users") will be individually assigned unique access identification accounts ("User ID") and passwords/passphrases (this also applies to the unique Server-to-Server access IDs and passwords/passphrases). Experian's approval of requests for (Internet) access may be granted or withheld in its sole discretion. Experian may add to or change its requirements for granting (Internet) access to the services at any time (including, without limitation, the imposition of fees relating to (Internet) access upon reasonable notice to Company), and reserves the right to change passwords/passphrases and to revoke any authorizations previously granted. *Note: Partially completed forms and verbal requests will not be accepted.*
4. An officer of the Company agrees to notify Experian in writing immediately if it wishes to change or delete any employee as a Head Security Designate, Security Designate, or Authorized User; or if the identified Head Security Designate, Security Designate or Authorized User is terminated or otherwise loses his or her status as an Authorized User.

Roles and Responsibilities

1. Company agrees to identify an employee it has designated to act on its behalf as a primary interface with Experian on systems access related matters. This individual shall be identified as the "Head Security Designate." The Head Security Designate can further identify a Security Designate(s) to provide the day to day administration of the Authorized Users. Security Designate(s) must be an employee and a duly appointed representative of the Company and shall be available to interact with Experian on information and product access, in accordance with these Experian Access Security Requirements. The Head Security Designate Authorization Form must be signed by a duly authorized representative of the Company. Company's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Company's Head Security Designate. The Head Security Designate will submit all requests to create, change or lock Security Designate and/or Authorized User access accounts and permissions to Experian's systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to Experian immediately.
2. As a Client to Experian's products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Company.
3. The Security Designate may be appointed by the Head Security Designate as the individual that the Company authorizes to act on behalf of the business in regards to Experian product access control (e.g. request to add/change/remove access). The Company can opt to appoint more than one Security Designate (e.g. for backup purposes). The Company understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with Experian's Security Administration group on information and product access matters.
4. The Head Designate shall be responsible for notifying their corresponding Experian representative in a timely fashion of any Authorized User accounts (with their corresponding privileges and access to application and data) that are required to be terminated due to suspicion (or actual) threat of system compromise, unauthorized access to data and/or applications, or account inactivity.

Designate

1. Must be an employee and duly appointed representative of Company, identified as an approval point for Company's Authorized Users.
2. Is responsible for the initial and on-going authentication and validation of Company's Authorized Users and must maintain current information about each (phone number, valid email address, etc.).
3. Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized User's job responsibilities.
4. Is responsible for ensuring that Company's Authorized Users are authorized to access Experian products and services.
5. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Company.
6. Must immediately report any suspicious or questionable activity to Experian regarding access to Experian's products and services.
7. Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to Experian.
8. Will provide first level support for inquiries about passwords/passphrases or IDs requested by your Authorized Users.
9. Shall be available to interact with Experian when needed on any system or user related matters.

_____ _____

Signature Date

_____ _____

Company Name Print Name/Title

Glossary

Term	Definition
Computer Virus	A Computer Virus is a self-replicating computer program that alters the way a computer operates, without the knowledge of the user. A true virus replicates and executes itself. While viruses can be destructive by destroying data, for example, some viruses are benign or merely annoying.
Confidential	Very sensitive information. Disclosure could adversely impact your company.
Encryption	Encryption is the process of obscuring information to make it unreadable without special knowledge.
Firewall	In computer science, a Firewall is a piece of hardware and/or software which functions in a networked environment to prevent unauthorized external access and some communications forbidden by the security policy, analogous to the function of Firewalls in building construction. The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.
Informati on Lifecycle	(Or Data Lifecycle) is a management program that considers the value of the information being stored over a period of time, the cost of its storage, its need for availability for use by authorized users, and the period of time for which it must be retained.
IP Address	A unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any All participating network devices - including routers, computers, time-servers, printers, Internet fax machines, and some telephones - must have its own unique IP address. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. It is important to keep your IP address secure as hackers can gain control of your devices and possibly launch an attack on other devices.
Peer-to-Peer	A type of communication found in a system that uses layered protocols. Peer-to-Peer networking is the protocol often used for reproducing and distributing music without permission.
Router	A Router is a computer networking device that forwards data packets across a network via routing. A Router acts as a junction between two or more networks transferring data packets.
Spyware	Spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the consent of that machine's owner or user. In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the internet.
Subscriber Code	Your seven digit Experian account number.
Experian Independent Third Party Assessment Program	The Experian Independent 3rd Party Assessment is an annual assessment of an Experian Reseller's ability to protect the information they purchase from Experian. EI3PA℠ requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Experian. EI3PA℠ also establishes quarterly scans of networks for vulnerabilities.
ISO 27001 /27002	IS 27001 is the specification for an ISMS, an Information Security Management System (it replaced the old BS7799-2 standard) The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
SSAE 16 SOC 2, SOC3	Statement on Standards for Attestation Engagements (SSAE) No. 1 SOC 2 Report on Controls Related to Security, Availability, Processing Integrity, Confidentiality, and Privacy. The SOC 3 Report , just like SOC 2, is based upon the same controls as SOC 2, the difference being that a SOC 3 Report does not detail the testing performed (it is meant to be used as marketing material).
FISMA	The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002.
CAI / CCM	Cloud Security Alliance Consensus Assessments Initiative (CAI) was launched to perform research, create tools and create industry partnerships to enable cloud computing assessments. The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.