374-S1511

Foster Youth Agency Membership Application

Experian

Experian Information Solutions Division

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

Business Information

Legal Name (under which tax returns are filed): County of El Dorado

DBA or Assumed Name: _____ Type of Agency: Government

Time in Business: _____ yrs _____ mos. Estimated # of Credit Reports Accessed Monthly: _____

Type of Agency: ☐ Federal ☐ State ☐ Municipality ☐ Tribal ☐ Other County

Government Website: www.edcgov.us Government Email Address: _____

Agency Physical Address (**no P.O. box numbers**): 3057 Briw Rd

City: Placerville, State: CA Zip: 95709 How Long? _____ yrs _____ mos.

Primary Phone: (530) 642-7300 Fax: ( ) _____ Is this a **residential** address? ☐ **Yes** ☒ **No**

Billing Address (if different): _____ City: _____ State: ___ ZIP: _____

Billing Contact: _____ Title: _____ Phone: ( ) _____

Permissible Purpose

(Application will not be processed unless this information is provided.)

Provide detailed description of your use of Experian products and consumer data. Also, describe the nature of your business interaction with consumers.
☒ Client will request and use the Services strictly in accordance with the federal Fair Credit Reporting Act, 15 U.S.C. 1681 *et seq.*, as amended (the "FCRA"), and for the sole purpose of complying with Section 106(b) of the CFSII, which requires Client to ensure that each child in foster care under its responsibility who has attained sixteen years of age does receive a copy of his or her consumer report each year until the child is discharged from foster care, and for complying with any applicable state laws addressing the same issue.

Head Designate for Internet Access

Full Name & Title: Jasan Burne, Security officer Email Address: jasan.burne@edcgov.us

Phone Number: (530) 621-5410 Signature (if different from below): Jasan B

User ID - First Choice (minimum 6 characters) jburne

User ID - Second Choice (minimum 6 characters) jaburne

User ID - Third Choice (minimum 6 characters) jasburne

Head Designate Certificate. If access to Experian services will occur via the Internet, Company agrees to identify an individual (the "Head Security Designate") that will act on behalf of Company for the purpose of submitting all requests to create, change or lock designate and/or end user access accounts and permissions to Experian systems and information via the Internet. For purposes of assigning a Head Security Designate, an agent is the same as the Company. Company certifies that the designate(s) is an authorized representative of Company's business and will be available to interact with Experian on information and product access matters, in accordance with Experian's Security Guidelines ("Guidelines"). Company acknowledges that the Guidelines may be updated from time to time by Experian and will be communicated to Company in writing. Company acknowledges and agrees that Company (a) has received a copy of the Guidelines, (b) has read and understands Company's obligations described in the Guidelines, (c) 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 (d) will abide by the provisions of the Guidelines when accessing Experian data via the Internet. Changes in Head Security Designate status (e.g., transfer or termination) are to be reported to Experian immediately.

I have read and understand the **"FCRA Requirements"** notice and Experian's **"Access Security Requirements"** and will take all reasonable measures to enforce them within my facility. I certify that I will use the Experian product information for no other purpose other than what is stated in the Permissible Purpose section on this application and for the type of business listed on this application. I will not sell the report to any consumer directly or indirectly. I understand that if my system is used improperly by Agency personnel, or if my access codes are made available to any unauthorized personnel due to carelessness on the part of any employee of this agency, I may be held responsible for financial losses, fees, or monetary charges that may be incurred and that my access privilege may be terminated.

Important Tax Notice
If Company is exempt from sales tax in any of the states where the information is delivered to you or accessed by you, please send Experian a completed and signed sales tax exemption certificate for each of those states.

I certify that I have read the above statements and all information provided is accurate.

County of El Dorado
Legal Agency Name

DBA Name (If Applicable)

X _____
Authorized Signature

Date

Brian Veerkamp,
Type or Print Name of Authorized Signer

Chair, Board of Supervisors
Title

If you have questions or need additional information, please call 1-800-831-5614.

EXPERIAN
AGREEMENT FOR CREDIT REPORTS
FOR FOSTER YOUTH

This Standard Terms and Conditions ("Agreement") is made on the Effective Date set forth below between Experian Information Solutions, Inc. and ("Experian") and County of El Dorado ("Client"). All references herein to this Agreement, unless otherwise specified, shall include the exhibits to this Agreement.

1. Agreement. This Agreement contains the standard terms and conditions for Experian's provision to Client of electronic access to consumer reports regarding certain foster children under Client's responsibility in accordance with Section 106(b) of the federal Child and Family Services Improvement and Innovation Act ("CFSII"), 42 U.S.C. 675(5) and/or similar state laws.

2. Term. The term of this Agreement shall begin upon the Effective Date set forth below and shall continue in effect until the termination in accordance with Section 13 of this Agreement.

3. Client Orders. Client shall provide Experian with such information as necessary to provide the Services, which shall include at Experian's request job specifications or criteria reasonably necessary to perform the Services ("Client Order"). The terms of this Agreement shall be superior to, and supersede, any conflicting or inconsistent terms contained in any Client Order or other Client provided documents. If Client changes or cancels a Client Order, or any portion thereof, after Experian has commenced work, Client agrees to pay Experian for its costs incurred for such work in process. If the Services are substantially completed at the time of such change or cancellation, Client agrees to pay Experian the full price for such Services.

4. FCRA Use. Client will request and use the Services strictly in accordance with the federal Fair Credit Reporting Act, 15 U.S.C. 1681 *et seq.*, as amended (the "FCRA"), and for the sole purpose of complying with Section 106(b) of the CFSII, which requires Client to ensure that each child in foster care under its responsibility who has attained sixteen years of age does receive a copy of his or her consumer report each year until the child is discharged from foster care, and for complying with any applicable state laws addressing the same issue.

5. Data Use Restrictions. Client agrees that it will not, either directly or indirectly, itself or through any agent or third party, without the prior written consent of Experian, request, compile, store, maintain, resell or use the Services (including any of the information contained in the Services) to build its own credit reporting database. Client shall be solely responsible for assuring the secure and confidential manner in which it stores, delivers and transmits Services to its authorized employee users. Client shall, at a minimum, comply with Experian's standard access security requirements a copy of which is attached to and incorporated into this Agreement as Exhibit A.

6. Inquiries. When accessing Services, Client certifies it will use reasonable measures to identify consumers and will accurately provide Experian with complete identifying information about the consumer inquired upon in the form specified by Experian. Client will enter all requested Client and type code information when requesting Services. Experian may use Client's inquiry data for any purpose consistent with applicable federal, state and local laws, rules, and regulations. Client will be responsible for installing the necessary equipment, software and security codes to prevent unauthorized access to an Experian database.

7. Third Party Processors/Agent. In the event Client chooses to use a third party to access the Services and fulfill Client's obligations under CFSII and/or applicable state laws addressing the same issue, . the parties understand and acknowledge that the third party shall be acting on behalf of Client. Client will cause the third party to (i) handle, process, and possess all Experian provided data in accordance with this Agreement, and (ii) sign a Third Party Processor Undertaking form or an Agency Addendum to this Agreement. Client shall provide Experian with the appropriate mailing instructions at least ten (10) days prior to the requested shipment date.

8. Data Blocking Service

(a) Data Contribution. If Client elects to use or test Experian's foster youth data blocking service, Client agrees to provide personal identification information (including full name, Social Security number, and date of birth) for the individual foster children for whom it seeks to prevent the creation of an Experian credit report until the foster child has reached the age of eighteen ("Client Records"). Client shall provide Records which are accurate to the best of its knowledge and shall promptly update and correct all known inaccurate information. At Experian's request, Client will promptly verify the accuracy of Client Records provided to Experian. Client shall bear the expense of preparing and delivering Client Records to Experian. Experian may, at its option and expense, incorporate Client Records into its credit reporting system. Once this information is incorporated into Experian's credit reporting system, this information will become Experian's exclusive property. Notwithstanding the foregoing, however, Client shall retain its interest in its Client Records in its original form and format.

(b) Experian Use. Experian may use Client Records provided by Client for the sole purpose of creating or testing a block of the creation of a credit report for foster youth.

9. Fees and Payment. The Services described in this Agreement will be provided by Experian to the Client at no charge to the Client.

10. Confidential Treatment. Under no circumstances will Client resell or otherwise disclose to any other person, other than employees or agents whose duties reasonably relate to the lawful business purpose for which the Services were obtained, any of the Services or data that Experian delivers to Client. Both parties hereby acknowledge that the Services and/or data provided by either party to the other may include personal information pertaining to individual consumers, and requires that the parties treat such information responsibly and take reasonable steps to maintain appropriate confidentiality and to prevent unlawful dissemination or misuse by its employees, officers, agents or any other person with access to such information. The Services and data shall only be used as expressly authorized in this Agreement.

11. Compliance with Laws. Experian shall comply with all federal, state and local laws, rules, regulations and decisions applicable to Experian's provision of Experian data and the Services pursuant to this Agreement. Client shall comply with all federal, state and local laws, rules regulations and decisions applicable to Client's collection and provision to Experian of the Client data and Client's use of the Experian data and Services provided pursuant to this Agreement. Experian reserves the right to revise the terms, or conditions or pricing under this Agreement, any Schedule and/or the Services (including without limitation the right to withdraw or restrict affected data) to meet any requirement imposed by federal, state, or local law, rule or regulation, or to address matters concerning privacy and confidentiality, upon reasonable notice to Client.

A. Security of Data. Client 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 Client's size and complexity, the nature and scope of its activities, and the sensitivity of the information provided to Client by Experian. 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 Experian, (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. Client shall provide its security program to Experian upon request and shall adopt any safeguard that Experian may reasonably request.

12. Data and Intellectual Property Ownership. Client acknowledges that Experian has expended substantial time, effort and funds to create and deliver the Services and compile its various databases. All data in Experian's databases and any other intellectual property that are part of the Services are and will continue to be Experian's exclusive property. Nothing contained in this Agreement or in any Schedule shall be

deemed to convey to Client or to any other party any ownership interest in or to intellectual property or data provided in connection with the Services provided however, Experian hereby grants Client a limited, non-exclusive, non-transferable, non-sublicenseable, license to use the data and Services for its own internal business purposes in accordance with the terms and conditions of this Agreement, and applicable law..

13. Termination.

A. Convenience. Either party may terminate this Agreement for its convenience upon thirty (30) days prior written notice to the other party.

B. Cause. If either party is in material breach of this Agreement, the non-breaching party may terminate the Agreement, as applicable, provided such breach is not cured within thirty (30) days following written notice of such breach, unless such breach is the failure to pay for the Services under the terms of this Agreement, in which case Client shall have ten (10) business days to cure such breach following notice.

C. Notwithstanding the foregoing, this Agreement may be terminated by Experian immediately upon written notice to Client if in Experian's reasonable good faith judgement any Services and/or data provided to Client are being used or disclosed contrary to this Agreement.

D. In the event that this Agreement is terminated as a result of a breach, the non-breaching party shall, in addition to its rights of termination, be entitled to pursue all other remedies against the breaching party.

E. Termination of this Agreement shall not relieve Client of its obligation to pay for any Services performed or provided by Experian under this Agreement or any Schedule.

F. Termination of this Agreement will only terminate Client's electronic access to consumer reports. Client will retain the ability to obtain paper copies of consumer reports relating to foster children under its responsibility, by submitting written requests by mail to Experian in accordance with Experian's policies, in order to fulfill Client's obligations under CFSII or applicable state laws.

14. Warranty and Disclaimers. Experian warrants to Client that Experian will use commercially reasonable efforts to deliver the Services in a timely manner. Because the Services involve conveying information provided to Experian by other sources, Experian cannot and will not, for the fee charged for the Services, be an insurer or guarantor of the accuracy or reliability of the Services or the data contained in its various databases. THE WARRANTY IN THE FIRST SENTENCE OF THIS PARAGRAPH IS THE ONLY WARRANTY EXPERIAN HAS GIVEN CLIENT WITH RESPECT TO THE SERVICES. EXPERIAN MAKES NO REPRESENTATION OR WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE SERVICES, ANY EXPERIAN DATA, OR ANY OTHER MATERIALS (TANGIBLE OR INTANGIBLE) SUPPLIED BY EXPERIAN HEREUNDER, AND EXPERIAN HEREBY EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTIES WITH RESPECT THERETO, INCLUDING WITHOUT LIMITATION, ANY WARRANTIES AS TO THE ACCURACY, COMPLETENESS OR CURRENTNESS OF ANY DATA OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.

15. Head Designate Certificate. Client agrees to identify, on Client's Membership Application, an individual (the "Head Security Designate") that will act on the behalf of Client for the purpose of submitting all requests to create, change or lock designate and/or end user access accounts and permissions to Experian systems and information via the Internet. Client certifies that the designate(s) is an authorized representative of Client and will be available to interact with Experian on information and product access matters, in accordance with Experian's Security Guidelines ("Guidelines"), a copy of which will be provided to Client with Client's membership welcome package. Client acknowledges that the Guidelines may be updated from time to time by Experian and will be communicated to Client in writing. Client acknowledges and agrees that Client (a) has received a copy of the Guidelines, (b) has read and understands Client's obligations described in the Guidelines, (c) will communicate the contents of the Guidelines, and any subsequent updates thereto, to all employees and agents that shall have access to Experian Services via the Internet, and (d) will abide by the provisions of the Guidelines when accessing Experian data via the Internet.

16. Limitation of Liability. Client acknowledges that Experian maintains several databases updated on a periodic basis, and that Experian does not undertake a separate investigation for each inquiry or request for Services made by Client. Client also acknowledges that the prices Experian charges for the Services are based upon Experian's expectation that the risk of any loss or injury that may be incurred by use of the Services will be borne by Client and not Experian. Client therefore agrees that it is responsible for determining that the Services are in accordance with Experian's obligations under this Agreement. If Client reasonably determines that the Services do not meet Experian's obligations under this Agreement, Client shall so notify Experian in writing within thirty days after receipt of the Services in question. Client's failure to so notify Experian shall mean that Client accepts the Services as is. If Client so notifies Experian within thirty days after receipt of the Services, then, unless Experian reasonably disputes Client's claim, Experian shall, at its option, either reperform the Services in question or issue Client a credit for the amount Client paid to Experian for the nonconforming Services. EXPERIAN'S REPERFORMANCE OF THE SERVICES OR THE REFUND OF ANY FEES CLIENT HAS PAID FOR SUCH SERVICES SHALL CONSTITUTE CLIENT'S SOLE REMEDY AND EXPERIAN'S MAXIMUM LIABILITY UNDER THIS AGREEMENT. IF NOTWITHSTANDING THE ABOVE, LIABILITY IS IMPOSED ON EXPERIAN, THEN CLIENT AGREES THAT EXPERIAN'S TOTAL LIABILITY FOR ANY OR ALL OF CLIENT'S LOSSES OR INJURIES FROM EXPERIAN'S ACTS OR OMISSIONS UNDER THIS AGREEMENT, REGARDLESS OF THE NATURE OF THE LEGAL OR EQUITABLE RIGHT CLAIMED TO HAVE BEEN VIOLATED, SHALL NOT EXCEED THE AMOUNT PAID BY CLIENT TO EXPERIAN UNDER THIS AGREEMENT FOR THE PARTICULAR SERVICES WHICH ARE THE SUBJECT OF THE ALLEGED BREACH DURING THE SIX MONTH PERIOD PRECEDING THE ALLEGED BREACH BY EXPERIAN. CLIENT COVENANTS THAT IT WILL NOT SUE EXPERIAN FOR ANY AMOUNT GREATER THAN SUCH AMOUNT.

NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY INCIDENTAL, INDIRECT, CONSEQUENTIAL, PUNITIVE OR SPECIAL DAMAGES (INCLUDING BUT NOT LIMITED TO DAMAGES TO BUSINESS REPUTATION, LOST BUSINESS, OR LOST PROFITS), WHETHER FORESEEABLE OR NOT AND HOWEVER CAUSED, EVEN IF SUCH PARTY IS ADVISED OF THE POSSIBILITY THAT SUCH DAMAGES MIGHT ARISE.

17. Waiver. Either party may waive compliance by the other party with any covenants or conditions contained in this Agreement or any Schedule, but only by written instrument signed by the party waiving such compliance. No such waiver, however, shall be deemed to waive any other circumstance or any other covenant or condition not expressly named in the written waiver.

18. Audit. Experian will have the right, upon at least ten (10) business days prior written notice, during Client's normal business hours and at Experian's expense, to audit Client's and any of its agent's use of the Services to assure compliance with the terms of this Agreement, if Experian has a good faith reason to believe the Client has not been, or may not be, in compliance with the terms of this Agreement. Client will be responsible for assuring full cooperation with Experian in connection with such audits and will provide Experian or obtain for Experian access to such properties, records and personnel as Experian may reasonably require for such purpose. Experian shall comply with those of Client's reasonable security policies provided reasonably in advance of any such audit. If an audit of the Client's use of the Services under this Agreement is not permitted by the Client, then Experian shall provide to Client, in writing stating where Client is non-compliant with its obligations under this Agreement and Experian will also request that Client give to Experian an adequate written assurance that it has corrected the problem and is otherwise complying with the terms of this Agreement. Experian shall be permitted, at its sole option and election, and without liability to the Client, to suspend or terminate the Services until such time as

Experian receives such adequate written assurance to Experian in writing. If adequate written assurance cannot be provided to Experian, then Experian shall be permitted to terminate this Agreement in accordance with Section 13 of this Agreement.

19. Successors and Assigns. This Agreement will be binding upon and will inure to the benefit of the parties hereto and their respective heirs, representatives, successors and permitted assignees. This Agreement may not be assigned, transferred, shared or divided in whole or in part by either party without other party's prior written consent, which consent shall not be unreasonably withheld.

20. Excusable Delays. Neither party shall be liable for any delay or failure in its performance under this Agreement (except for the payment of money) if and to the extent which such delay or failure is caused by events beyond the reasonable control of the party including, without limitation, acts of God, public enemies, or terrorists, labor disputes, equipment malfunctions, material or component shortages, supplier failures, embargoes, rationing, acts of local, state or national governments or public agencies, utility or communication failures or delays, fire, earthquakes, flood, epidemics, riots and strikes. If a party becomes aware that such an event is likely to delay or prevent punctual performance of its own obligations, the party will promptly notify the other party and use its best effort to avoid or remove such causes of nonperformance and to complete delayed job whenever such causes are removed.

21. Choice of Law. This Agreement is governed by and construed in accordance with the internal substantive laws of the _____ (Insert name of State). Any dispute under this Agreement shall be brought in the federal or state courts in _____ County (insert applicable county), _____ (insert Name of State).

22. Notices. All notices, requests and other communications hereunder shall be in writing and shall be deemed delivered at the time of receipt if delivered by hand or communicated by electronic transmission, or, if mailed, three (3) days after mailing by first class mail with postage prepaid. Notices to Experian and Client shall be addressed to the addresses provided below each party's signature, or to such other address as either party shall designate in writing to the other from time to time.

23. Complete Agreement. This Agreement, , sets forth the entire understanding of Client and Experian 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.

24. Amendments. This Agreement may only be amended in writing signed by authorized representatives of both parties.

25. Survival. The provisions of Sections 4, 5, 6, 7, 9, 10, 11, 14, 15, 16 and 18, in addition to any other provisions of this Agreement or any Schedule that would normally survive termination, shall survive termination of this Agreement for any reason.

25. Authority to Sign. Each party represents that (i) the person signing this Agreement has all right, power and authority to sign this Agreement on behalf of such party; and (ii) such party has full power and authority and all necessary authorizations to comply with the terms of this Agreement and to perform such party's obligations under this Agreement.

IN WITNESS WHEREOF, Client and Experian sign and deliver this Agreement as of the Effective Date set forth below.

Experian Information Solutions, Inc.

By: _____
Signature (Duly Authorized Representative Only)

Name: _____
Print

Title: _____

Effective Date: _____

Address for Notice: Experian Information Solutions, Inc., 475 Anton Boulevard, Costa Mesa, CA 92626, Attn: General Counsel

County of El Dorado
Print or Type Legal Name of Company

By: _____
Signature (Duly Authorized Representative Only)

Name: Brian Veerkamp
Print

Title: Chair, Board of Supervisors

Physical Address for Notice: 3057 Briw Rd, Placerville, CA 95709
Attn: Attn: CPS Analyst

The County Officer or employee with responsibility for administering this Agreement is Mark Contois, Program Manager II, or successor.

Experian

Access Security Requirements
for FCRA and GLB SA 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. <u>Maintain an Information Security Policy</u>

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 Internet Security Guidelines. 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.

Experian

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.
Information 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.