CIC
The Power of Decision™

FCRA and Access Security Requirements / CIC Policies

IMPORTANT: PLEASE READ CAREFULLY!

We must work together to protect the privacy and information of consumers. The following information security measures are designed to reduce unauthorized access to consumer information. It is your responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to employ an outside service provider to assist you.. The credit reporting agency reserves the right to make changes to Access Security Requirements without notification. The information provided herewith provides minimum baselines for information security. ***In accessing the credit reporting agency's services, you agree to follow these security requirements.*** These requirements are applicable to all systems and devices used to access, transmit, process, or store Experian, TransUnion, and Equifax data:

1. Implement Strong Access Control Measures

1.1 Do not provide your credit reporting agency Subscriber Codes or passwords to anyone. No one from the credit reporting agency will ever contact you and request your Subscriber Code number or password.

1.2 Proprietary or third party system access software must have credit reporting agency Subscriber Codes and password(s) hidden or embedded. Account numbers and passwords should be known only by supervisory personnel.

1.3 You must request your Subscriber Code password 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.

1.4 Protect credit reporting agency Subscriber Code(s) and password(s) so that only key personnel know this sensitive information. Unauthorized personnel should not have knowledge of your Subscriber Code(s) and password(s).

1.5 Create a separate, unique user ID for each user to enable individual authentication and accountability for access to the credit reporting agency's infrastructure. Each user of the system access software must also have a unique logon password.

1.6 User IDs and passwords must not be shared, posted, or otherwise divulged in any manner. Restrict the number of key personnel who have access to credit information.

1.7 Keep user passwords Confidential.

1.8 Develop strong passwords that are: not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers &letters); contain a minimum of eight (8) alpha/numeric characters for standard user accounts; for interactive sessions (i.e. non system-to-system) ensure that passwords are changed periodically (every 90 days is recommended)

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 your membership application.

1.13 Subscriber must not install Peer-to-Peer file sharing software on systems used to access, transmit or store credit data.

1.14 Ensure that you and your employees **do not access your 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 credit reporting agency 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 your 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 (laptop and desktop) and all other systems current with appropriate system patches and updates.

2.2 Configure infrastructure such as Firewalls, Routers, personal computers (laptops and desktops), and similar components to industry best security practices, including disabling unnecessary services or features, 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 computer virus detection/scanning product on all computers, systems and networks 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.

• If you suspect an actual or potential virus, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

• 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.

2.4 Implement and follow current best security practices for computer anti-Spyware scanning services and procedures:

• Use, implement and maintain a current, commercially available computer anti-Spyware scanning product on all computers, systems and networks.

• If you suspect actual or potential Spyware, immediately cease accessing the system and do not resume the inquiry process until the problem has been resolved and eliminated.

• Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from your computers.

• Keep anti-Spyware software up-to-date by vigilantly checking or configuring auto updates and installing new anti-Spyware definition files weekly, at a minimum. If your company's computers have unfiltered or unblocked access to the Internet (which prevents access to some known problematic sites), then it is recommended that anti-Spyware scans be completed more frequently than weekly.

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 All credit reporting agency data is classified as Confidential and must be secured to this requirement 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 credit reporting agency data and information when stored electronically on any system including but not limited to laptops, computers, tablets, servers, databases using strong encryption such as AES 256 or above

3.5 Credit 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 credit data, ensure that such devices are protected via device pass-code.

3.7 Applications utilized to access all credit 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 credit 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 credit 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 Safeguard 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 credit data may have been compromised, immediately notify CIC within twenty-four (24) hours.

4.4 The FACTA Disposal Rules requires that you 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. Telephone notification is preferred (800)288-4757, Email notification will be sent to compliance@cicreports.com.

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

4.6 When using third party service providers (e.g. application service providers) to access, transmit, store or process credit 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 Subscribers responsibility to ensure the service provider is engages with Experian and exception is granted in writing.

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

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

5.5 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.

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

5.7 For wireless networks connected to or used for accessing or transmission of credit 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.

5.8 When using service providers (e.g. software providers) to access Experian, TransUnion, or Equifax data, access to third party tools/services must require multi-factor authentication.

5.9 CIC reserves the right to audit the security mechanisms of the Subscriber to safeguard access to bureau information, systems and electronic communications. Audits may include examination of system security and associated administrative practices.

6. Regularly Monitor and Test Networks

6.1 Perform regular tests on information systems (port scanning, virus scanning, 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 In cases where the Subscriber is accessing bureau information and systems via third party software, the Subscriber agrees to make available to CIC upon request, audit trail information and management reports generated by the vendor software, regarding Subscriber individual Authorized Users.

6.3 Use current best practices to protect your telecommunications systems and any computer system or network device(s) you use to provide Services hereunder to access CIC 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. Subscriber shall be responsible for and ensure that third party software, which accesses bureau 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.

6.4 Subscriber shall report actual security violations or incidents that impact consumer information to CIC within twenty-four (24) hours. Subscriber agrees to provide notice to CIC 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 800-288-4757, Email notification will be sent to compliance@cicreports.com .

7. Mobile and Cloud Technology

7.1 Storing credit data on mobile devices is prohibited.

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 and all other 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.

7.4 Mobility solution and all other software server/systems 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 credit 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 credit 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 credit 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: ISO 27001, PCI DSS, EI3PA, SSAE 16 – SOC 2 or SOC3, FISMA, CAI / CCM assessment.

8. FCRA & Other Policies

8.1 You must always get a subject's written authorization before accessing their credit and/or public record profile. If you access a subject's credit and/or public record information under false pretenses, and/or without their authorization the penalty for such action(s) under the Federal FCRA Section 621(a)(2)(A) is imprisonment for up to one year and up to a $3,500 fine per violation, and/or any civil damages the court may award the party which brought the action. ***EXCEPTION:*** **The Federal Fair Credit Reporting Act states in effect that a creditor or their authorized agent attempting to collect a valid and legally enforceable debt (with or without a judgment) from a subject, can obtain a credit profile on that subject without their authorization.**

8.2. Record Retention – The Federal Equal Opportunities Act states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the FCRA/FACTA, the credit reporting agency requires that you **retain the credit/rental application for a period of not less than 6 years (both approved and denied applicants).** When conducting an investigation, particularly following a breach or a consumer complaint that your company impermissibly accessed their credit report, the credit reporting agency 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.

8.3 Adverse Action - If you deny a subject for a credit related transaction (in the form of a rental of a dwelling, the financing of a product or service, etc.) you are to provide them with such a notice in writing. This notice must reference that CRA's name, address and toll free number that provided the report and the CRA did not make the decision to take adverse action. State that the subject can request a copy of their credit profile from the credit reporting agency in question free of charge. They must request their credit profile within 60 days from the date they were denied credit (otherwise, they must pay the credit bureau's prevailing rate for a copy of their report). In addition, the notice must state that the subject has the right to dispute the accuracy or completeness of any information contained in their consumer credit and/or public record report.

8.4 Prohibited Businesses -CIC cannot serve any companies or individuals engaged in any of the following businesses: adult entertainment, businesses in an unrestricted residential location, attorneys or law offices, bail bondsman, check cashing, credit counseling or repair, dating service, financial counseling, genealogical research and people locator service, massage service, pawn shop, private detectives, 3rd party repossession, companies involved in spiritual counseling, future services (ex. health club, timeshare), tattoo service, news agencies, insurance claims, those who intend to re-sell its credit and/or public record reports directly, or indirectly, or those who plan to use (or which do use) such information in any unlawful manner as set forth in the Fair Credit Reporting Act, as well as any other applicable federal, state, and/or local laws(s). Furthermore, CIC cannot serve any individuals or companies which plan to use (or which do use) its reports for any purpose(s) prohibited by its policies and/or agreement. If you misuse said information in the manner(s) described above, your account with CIC will be terminated without notice.

8.5 Death Master File

Subscriber acknowledges that many services containing credit 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 credit bureau information, the subscriber's use of deceased flags or other indicia within the credit 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 the subscriber 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 credit information.

Subscriber has read and understands the **"FCRA and Access Security Requirements/CIC Policies"** and will take all reasonable measures to enforce them. Subscriber acknowledges receipt of a copy of these requirements, and will communicate the contents of the applicable requirements to all employees that will have access to CIC services, systems or data.

Subscriber understands that its use of CIC networking and computing resources may be monitored and audited, without further notice.

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

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