INTERNET SECURITY REQUIREMENTS

These Internet Security Requirements ("Internet Security Requirements") are made with reference to the Agreement for Service between CREDCO and Client. Capitalized terms used, but not otherwise defined, herein are used with the meanings assigned to such terms in the Agreement for Service. Client agrees that it and all third parties accessing Services on Client's behalf (referred to collectively herein as "Client") will comply with the following requirements in connection with ordering and receiving Information Services through the Internet:

1. **General.**

a. CREDCO will provide Client subscriber codes, security digits, access codes, telephone access numbers and other proprietary information to enable Client to access the Information Services through the Internet (together, "CREDCO Access Information"). CREDCO reserves the right to change the CREDCO Access Information (or any item or items thereof) periodically and/or at any time, effective upon notice to Client.

b. For purposes of these Internet Security Requirements, the information in the Information Services and the CREDCO Access Information are sometimes referred to, together, as "CREDCO Information."

c. Client shall have Information Security policies and procedures in place that are consistent with the practices described in an industry standard, such as ISO 27002 and/or this Internet Security Requirements, which is aligned to applicable laws and regulations, and Credco's Vendor's requirements, including Experian's Information Security policy.

2. **Data Security.**

a. All CREDCO Information and consumer identifying information must be encrypted in storage and in transit as it is delivered through the Internet. 256-bit TLS or higher strength encryption is required.

b. Encrypt all consumer credit bureau data when stored electronically on any system including but not limited to laptops, tablets, personal computers, servers, databases using strong encryption such as AES 256 or above.

c. All CREDCO Information must be protected when stored on servers, subject to at least the following requirements:

i. Servers storing CREDCO Information must be separated by a firewall or other comparable method from publicly accessible web-servers;

ii. CREDCO Information must not be on a server that can be accessed by TCP services directly from the Internet and must not be referenced in domain name services (DNS) tables;

iii. All security access to these servers, both physical and network, must include authentication and, in the case of network security, passwords that are changed at least once every 90 days; and

iv. All servers must be kept current with all operating system patches, as they become available.

d. CREDCO Information may not be shared with, or accessed by any person other than an Authorized Employee (as defined in paragraph f. below). All transmission and/or storage of CREDCO Information is subject to all the terms and conditions contained in these Internet Security Requirements.

e. When displaying any nonpublic information in HTML, no CREDCO Information can be stored on the presentation server(s). Client will use the presentation server(s) only to receive the HTTP services. All HTML shall be dynamically created or interpreted by the application server. The presentation server(s) shall only receive the data and process it back and forth to the application server. Data transmitted between Client's browser and the application server must not be cached, in any form, on the presentation server(s).

f. Only Authorized Employees shall have computer network or terminal or any other access to any CREDCO Information. Authorized Employees are employees of Client who have a need to access CREDCO Information in order to carry out their official duties with Client for the purposes specified in the Agreement for Service. Prior to providing an Authorized Employee with access to any CREDCO Information, Client will provide the Authorized Employee with adequate training regarding the Internet Security Requirements and will require the Authorized Employee to agree to comply with all such requirements. Client will not add any employee as an Authorized Employee unless the employee has received the required training and has agreed to comply with the Employee Requirements.

g. Client shall implement adequate security measures in order to prevent use or access of CREDCO Information by persons other than Authorized Employees, including, without limitation, the following: (i) assigning each Authorized Employee a unique Internet identification and password (together, "Operator Passwords"), (ii) changing the Operator Passwords at least once every ninety (90) days or sooner if a specific Authorized Employee is no longer responsible for accessing CREDCO Information or Client has learned or suspects that there has been unauthorized access to an Operator Password, (iii) limiting knowledge of the CREDCO Access Information and Operator Passwords to Authorized Employees and strictly prohibiting the sharing, disclosure, or public display of any such information, (iv) using all security features in the software and hardware used to access CREDCO Information, (v) not transferring any hardware or software between locations without deletion of all CREDCO Access Information and Operator Passwords, and (vi) if unauthorized access to CREDCO Access Information is discovered or suspected, immediately notifying CREDCO and further undertaking all remedial efforts within its power and control to cure such unauthorized access or use.

3. **Network Topology.**

a. Client will use security measures, including anti-virus software, to protect communications systems and networks device to reduce the risk of infiltration, hacking, access penetration by, or exposure to, an authorized third-party.

b. Client's Internet connection must be protected with dedicated, industry-recognized firewalls that are configured and managed to adhere to industry best practices.

c. CREDCO Information may be held only on a secure application server that can be accessed only by a secure presentation server, through one of the following methods:

i. Dual or multiple firewall protection (**preferred**): This method consists of a firewall between the Internet and the presentation server(s) and another firewall between the presentation server(s) and the application server holding the CREDCO Information. The network firewall should ensure that only the presentation server(s) is/are allowed to access the application server holding the CREDCO Information.

ii. Single firewall method (**acceptable**): When a dual firewall method is not feasible, a single firewall will provide acceptable levels of protection. The firewall should be installed between the Internet and the presentation server(s). Multiple interfaces to the separate presentation server (s) and the application server holding the CREDCO Information are required. The firewall should be configured to allow only the presentation server(s) access to the application server holding CREDCO Information.

d. All administrative access to the firewalls and servers should be through a secure internal network. Remote access must be configured so that the administrator dials into a LAN, is authenticated and verified, and then is granted access to the firewalls and servers from inside the network. No direct modem access should be available to the firewalls or servers.

e. No internal Internet Protocol (IP) addresses should be publicly available or natively routed to the Internet.
f. The network should not provide any access to any firewall or servers without proper strong authentication or through the firewalls.
g. Client shall have logging mechanisms in place sufficient to identify security incidents, establish individual accountability, and reconstruct events. Audit logs will be retained in a protected state (i.e., encrypted or locked) with a process for periodic review.
h. Any exceptions or alerts must be logged and reviewed by Client and maintained for at least one (1) year for review by CREDCO.
i. User identifiers and logon processes may not be transmitted in clear-text across internal or external network.

4. Client Authentication.

a. CREDCO will not provide any CREDCO Information to Client unless CREDCO is able to authenticate Client through a strong authentication methodology.
b. Client will log each access of Information Services (see section 3(g) above) and the identity of the specific Authorized Employee that made the access, and shall maintain such information for at least one (1) year for review by CREDCO.

5. Client Verification.

a. Once Client has been authenticated as describe above, CREDCO will verify the identity of Client through authentication and verification procedures that provide an acceptable level of security for access to Information Services.
b. At the present time, CREDCO requires verification through issuance by CREDCO, and use by Client, of a Client User ID and password. The initial password will be issued by CREDCO and not created by Client. Passwords will have a minimum of eight (8) characters in an alphanumeric combination and will be changed at least once every ninety (90). Passwords and User IDs will be encrypted with 128-bit encryption. All users are required to change passwords whenever there is any indication of possible system or password compromise. Passwords cannot be changed for a minimum of ten (10) days. The minimum password age must be set to 10 days on all systems.
c. The User IDs and passwords must be stored on a server protected by the security measures applicable to the CREDCO Information.
d. Client must ensure that all IDs of Authorized Employees who are no longer authorized to obtain CREDCO Information are disabled or revoked immediately.
e. Client must have procedures in place that create appropriate audit trails for all transactions.
f. CREDCO will protect Client access by timing out Client after a period of inactivity not to exceed thirty (30) minutes. CREDCO will also protect Client access by enforcing a limit of 5 consecutive invalid access attempts by a user during a 30 minute period. Passwords must not be the same for 5 consecutive times. The minimum password history must be set to 5 on all systems.

6. Change of Requirements.

CREDCO may, from time to time, change any of the requirements herein (including by imposing new requirements or procedures or modifying existing ones) by giving Client written notice of the change. Client will conform its systems, applications, processes, and procedures to comply with the change not later than the effective date specified by CREDCO in the notice, or if none is specified, thirty (30) days after receipt of the notice.

7. Prohibition of Oral Modification of Requirements.

No oral modification of these requirements will be permitted, and CREDCO must approve in writing any variance by Client.

8. Client Responsibility.

Compliance by Client with these requirements shall not relieve Client from the obligation to observe any other or further contractual, legal or regulatory requirements, nor shall CREDCO's review or approval of any of Client's systems, applications, processes, or procedures constitute or be deemed to constitute the assumption by CREDCO of any responsibility or liability for compliance by Client with any of the same. Client shall remain solely responsible for the security of its systems and the security of all CREDCO Information received by it from CREDCO and for any breach of that security. CREDCO retains the right, in its sole discretion, to withhold approval of Internet access to Information Services for any reason. CREDCO may suspend or terminate access to the CREDCO Information at any time if CREDCO has reason to believe that Client has violated any of these Internet Security Requirements or any contractual, legal, or regulatory requirements, rules or terms. **Client reaffirms that it will not transmit any Information Services (or information therein) through the Internet without express written permission of CREDCO.**