Access Security Requirements

The following information security controls are required to safeguard against unauthorized access to Experian, TransUnion, Equifax, and other information services that contain confidential consumer information; hereinafter referred to as "consumer report(s)". It is your (End User) responsibility to implement these controls. If you do not understand these requirements or need assistance in your compliance, it is your responsibility to get an outside service provider to assist you. Avantus 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 Avantus services, End User agrees to follow these security requirements. These requirements are applicable to all systems and devices used to access, transmit, process, or store consumer reports:

1. Implement Strong Access Control Measures

1.1 All credentials such as User names/identifiers/account numbers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party. No one from Avantus will ever contact you and request your credentials.

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

1.3 If the third party or third party software or proprietary system or software, used to access Avantus 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 Avantus 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 End User 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. user/account 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's (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 End User must NOT install Peer-to-Peer file sharing software on systems used to access, transmit or store consumer reports.

1.14 Ensure that End User 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 consumer reports 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 End User'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 Consumer reports are classified as Confidential and must be secured to in accordance with the requirements mentioned in this document at a minimum.

3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.

3.4 Encrypt all consumer reports and information when stored electronically on any system including but not limited to laptops, tablets, personal computers, servers, databases using strong encryption such AES 256 or above.

3.5 Consumer reports must not be stored locally on smart tablets and smart phones such as iPads, iPhones, Android based devices, etc.

3.6 When using smart tablets or smart phones to access consumer reports, ensure that such devices are protected via device pass-code.

3.7 Applications utilized to access consumer reports via smart tablets or smart phones must protect data while in transmission such as SSL protection and/or use of VPN, etc.

3.8 Only open email attachments and links from trusted sources and after verifying legitimacy.

3.9 When no longer in use, ensure that hard-copy materials containing consumer reports are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.

3.10 When no longer in use, electronic media containing consumer reports 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* consumer reports *may have been compromised, immediately notify Avantus within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).*

4.4 The FACTA Disposal Rules requires that End User 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 consumer reports, ensure that service provider is compliant with the Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian's list of compliant service providers. If the service provider is in the process of becoming compliant, it is End User's responsibility to ensure the service provider is engaged with Experian and an exception is granted in writing. Approved certifications in lieu of EI3PA are, ISO 27001/27002, PCI DSS, SSAE 16 SOC2, SOC3, FISMA, CAI/CCM.

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 consumer reports, 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 Avantus 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 consumer reports; 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 Avantus 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 consumer reports 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 can consumer reports 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 consumer reports 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 consumer reports, 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 – SOC2 or SOC3, FISMA, CAI/CCM Assessment.

8. **General**

8.1 Avantus may from time to time audit the security mechanisms End User maintains to safeguard access to consumer reports, systems and electronic communications. Audits may include examination of systems security and associated administrative practices

8.2 In cases where the End User is accessing consumer reports and systems via third party software, the End User agrees to make available to Avantus upon request, audit trail information and management reports generated by the vendor software, regarding End User individual authorized users.

8.3 End User shall be responsible for and ensure that third party software, which accesses Avantus 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 End User shall conduct software development (for software which accesses Avantus 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 Avantus systems shall be made available to Avantus upon request, for example during breach investigation or while performing audits

8.6 Data requests from End User to Avantus 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 End User shall report actual security violations or incidents that impact Experian, Equifax and/or TransUnion to Avantus within twenty-four (24) hours or per agreed contractual notification timeline. End User agrees to provide notice to Avantus 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 (800-243-0120 extension 107) Email notification will be sent to compliance@avantus.com.

8.8 In the event of a security incident, where as a consumers information has been compromises, (1) End User shall provide to each affected or potentially affected consumer, a credit history monitoring services for a minimum of one year. (2) Avantus may assess End User an expense recovery fee for those costs.

8.9 End User acknowledges and agrees that the End User (a) has received a copy of these requirements, (b) has read and understands End User'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 Avantus services, systems or data, and (d) will abide by the provisions of these requirements when accessing consumer reports.

8.10 End User understands that its use of Avantus networking and computing resources may be monitored and audited by Avantus, without further notice.

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

8.12 When using third party service providers to access, transmit, or store consumer reports, additional documentation may be required by Avantus.

"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, the following requirements apply where End User and their employees or an authorized agent/s acting on behalf of the End User are provided access to Avantus provided services via Internet ("Internet Access").

General requirements:

1. The End User shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with Avantus on systems access related matters. The End User's Head Security Designate will be responsible for establishing, administering and monitoring all End User employees' access to Avantus provided services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such functions.
2. The End User'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 Avantus product based upon the legitimate business needs of each employee. Avantus 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 End User shall request employee's (Internet) user access via the Head Security Designate/Security Designate in writing, in the format approved by Avantus. 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). Avantus approval of requests for (Internet) access may be granted or withheld in its sole discretion. Avantus 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 End User), 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 End User agrees to notify Avantus 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. End User agrees to identify an employee it has designated to act on its behalf as a primary interface with Avantus 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 End User and shall be available to interact with Avantus on information and product access, in accordance with these Access Security Requirements for Avantus End-Users. The Head Security Designate Authorization Form must be signed by a duly authorized representative of the End User. End User's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to End User'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 Avantus systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to Avantus immediately.
2. As a Client to Avantus products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of End User.
3. The Security Designate may be appointed by the Head Security Designate as the individual that the End User authorizes to act on behalf of the business in regards to Avantus product access control (e.g. request to add/change/remove access). The End User can opt to appoint more than one Security Designate (e.g. for backup purposes). The End User understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with the Avantus Security Administration group on information and product access matters.
4. The Head Designate shall be responsible for notifying their corresponding Avantus 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 End User, identified as an approval point for End User's Authorized Users.
2. Is responsible for the initial and on-going authentication and validation of End User'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 End User's Authorized Users are authorized to access Avantus products and services.
5. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by End User.
6. Must immediately report any suspicious or questionable activity to Avantus regarding access to Avantus products and services.
7. Shall immediately report changes in their Head Security Designates status (e.g. transfer or termination) to Avantus.
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 Avantus when needed on any system or user related matters.