

## Access Security Requirements

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. *We recognize that all of the items or terms identified in this document may not necessarily apply to each end user.* If you do not understand these requirements or need assistance, it is your responsibility to employ an outside service provider to assist you. Capitalized terms used herein have the meaning given in the Glossary attached hereto. Experian reserves the right to make changes to Access Security Requirements without notification. The information provided herewith provides a baseline 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 to access 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) 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)
- 1.8 Passwords (e.g. subscriber code passwords, user passwords) 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 algorithms 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 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.
- 1.14 Company must NOT install Peer-to-Peer file sharing software on systems used to access, transmit or store Experian data.
- 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 (laptop and desktop) 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, 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 of 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 All Experian data is classified as Confidential and must be secured 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 as AES 256 or above.
- 3.5 Experian data must not be stored locally on smart tablets and smart phones such as iPads, iPhones, Android based devices, etc.
- 3.6 When using smart tablets or smart phones to access Experian data, ensure that such devices are protected via device pass-code.
- 3.7 Applications utilized to access Experian data via smart tablets or smart phones must protect data while in transmission such as SSL protection and/or use of VPN, etc.
- 3.8 Only open email attachments and links from trusted sources and after verifying legitimacy.
- 3.9 When no longer in use, ensure that hard-copy materials containing Experian data are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.
- 3.10 When no longer in use, electronic media containing Experian data is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).

### **4. Maintain an Information Security Policy**

- 4.1 Develop and follow a security plan to protect the Confidentiality and integrity of personal consumer information as required under the GLB 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 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 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.
- 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 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 encryption (for example, IEEE 80211i) 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 tolls/services must require multi-factor authentication.

## **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 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 your telecommunications systems and any computer system or network device(s) you use 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. Regularly Monitor and Test Networks**

- 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 outsources 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](mailto: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 Opportunities 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 \$2,500 per violation.”*

Client Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Glossary

<b>Term</b>	<b>Definition</b>
<b>Computer Virus</b>	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.
<b>Confidential</b>	Very sensitive information. Disclosure could adversely impact your company.
<b>Encryption</b>	Encryption is the process of obscuring information to make it unreadable without special knowledge.
<b>Firewall</b>	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.
<b>Information Lifecycle</b>	(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.
<b>IP Address</b>	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.
<b>Peer-to-Peer</b>	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.
<b>Router</b>	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.
<b>Spyware</b>	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.
<b>SSID</b>	Part of the Wi-Fi Wireless LAN, a service set identifier (SSID) is a code that identifies each packet as part of that network. Wireless devices that communicate with each other share the same SSID.
<b>Subscriber Code</b>	Your seven digit Experian account number.
<b>Experian Independent Third Party Assessment Program</b>	The Experian Independent 3 <sup>rd</sup> 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.
<b>ISP 27001 / 27002</b>	IS 27001 is the specification for an ISMS, and 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.
<b>PCI DSS</b>	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle carholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
<b>SSAE 16 SOC 2, SOC3</b>	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).
<b>FISMA</b>	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.
<b>CAI / CCM</b>	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 provided fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.