



The Landlord Association of Pennsylvania

1414 Millard Street  
Bethlehem, PA 18018  
Tel. (610) 867-8940 ▪ Fax (610) 867-8604

# MEMBERSHIP APPLICATION

Date of Application: \_\_\_\_\_

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

## A. GENERAL COMPANY INFORMATION

**\*New Membership requires a "Site Inspection"**

Company Name: \_\_\_\_\_ Years in Business: \_\_\_\_\_

Type of Ownership: Indicate one  Partnership  Sole Owner  Nonprofit  Corporation

Other business name(s) or dba: \_\_\_\_\_ EIN Number: \_\_\_\_\_

Business Hours: Indicate one  8 am – 5 pm  9am – 6 pm  Other \_\_\_\_\_ Business Days:  M  T  W  TH  F  S  S

Have you previously applied or have been a LAPA Member  Yes  No If Yes, when? \_\_\_\_\_

Under what business name? \_\_\_\_\_

Physical Street Address (no P.O Box numbers please): \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_ How long: \_\_\_\_\_ Yrs \_\_\_\_\_ Mos. \_\_\_\_\_

Type of Property: Indicate one  Residential  Commercial Phone: ( ) \_\_\_\_\_ Fax: ( ) \_\_\_\_\_

## B. PRINCIPAL OF THE COMPANY: (If the sole owner or partnership please complete the next section below)

I understand that the information provided below will be used to obtain a consumer credit report, and my credit worthiness may be considered when making a decision to grant membership.

Principal Name: \_\_\_\_\_

Title or Position: \_\_\_\_\_ Phone: ( ) \_\_\_\_\_

Social Security Number: \_\_\_\_\_ Date of Birth: \_\_\_\_\_

Residential Street Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

## C. BUSINESS/LICENSE CONFIRMATION: (For security purposes, all new members are required to provide a minimum of THREE forms of ID for membership)

**D.**

<u>MUST HAVE</u>	<u>Pick 1 Additional Proof</u>
<input type="checkbox"/> Photo ID	<input type="checkbox"/> Copy of Landlord License
<input type="checkbox"/> Copies of 3 different signed Rental Applications	<input type="checkbox"/> Copy of Rental Property Title
	<input type="checkbox"/> Copy of Rental Tax Bills
	<input type="checkbox"/> Copy of Rental Insurance Documents

\*Documented verification must include: Name of Bank, Contact, Phone #, date & person conducting verification: \_\_\_\_\_

## D. BUSINESS INFORMATION: (Please tell us about your company)

Type of business: \_\_\_\_\_ Do you need a purchase order?  Yes  NO PO# \_\_\_\_\_

Do you have an Investigation License?  Yes  No If yes, please provide a copy with this application.

How many Credit Reports will you be accessing monthly? \_\_\_\_\_

How will you be accessing LAPA Credit Reports? (i.e. Internet, In Office) \_\_\_\_\_

Does your company qualify for tax exemptions?  Yes  No If yes, please provide proof.

## E. PERMISSABLE PURPOSE INFORMATION: (Application will not be processed unless this information is provided below)

Describe the specific purpose for which LAPA credit information will be used:

Screening prospective tenants

---

---

**F. BILLING ADDRESS:**

**Contact Name:** \_\_\_\_\_ **Phone:** \_\_\_\_\_  
**Address:** \_\_\_\_\_  
**City:** \_\_\_\_\_ **State:** \_\_\_\_\_ **Zip:** \_\_\_\_\_  
**County:** \_\_\_\_\_ **SIC #** \_\_\_\_\_

---

**BANKING REFERENCES:** *(Please provide the name of the bank which maintains your business checking account)*

**Bank:** \_\_\_\_\_ **Phone:** \_\_\_\_\_  
**Address:** \_\_\_\_\_  
**City:** \_\_\_\_\_ **State:** \_\_\_\_\_ **Zip:** \_\_\_\_\_  
**Business Checking Account:** \_\_\_\_\_

---

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

Member acknowledges that he/she has received and read a copy of the current Terms and Conditions of Membership for LAPA. LAPA reserves the right at anytime without notice, to amend the Terms and Conditions of Membership.  
MEMBER ACKNOWLEDGES AND ACCEPTS FULL RESPONSIBILITY AND GUARANTEES PAYMENT FOR ALL SERVICES RENDERED THROUGH LAPA.

Initial: \_\_\_\_\_

Member must notify LAPA immediately by telephone or writing if there internet passwords are lost or stolen. Member is responsible for all reports ordered under their company password. Failure to notify LAPA of the loss of your passwords may result in the posting of significant charges to the credit card account you identify on your application.

Initial: \_\_\_\_\_

Member agrees that LAPA may pursue all avenues of collection, including use of collection agencies, and authorizes LAPA to prepare and submit credit card charges using any/or all cards listed above to recover all charges and all unpaid accounts due.

Initial: \_\_\_\_\_

**Important Tax Notice**

Credit Reports are subject to sales tax for businesses located in the states of Pennsylvania and Maryland. If your company is located in one of these states and is tax exempt for any reason, please submit a statement of your tax exemption certificate along with this application. If you remit a use tax directly to the state, please submit a statement of use tax or a letter on your company letterhead which states that you pay use tax.

All replications of the Membership Application shall be deemed an original.

I certify that I have read the above statements and all information provided is accurate and hereby authorize the Bank & Business References to release information to LAPA.

\_\_\_\_\_  
Company Name

\_\_\_\_\_  
Type or Print Name and Title of Owner or Officer

\_\_\_\_\_  
Authorized Signature

\_\_\_\_\_  
Date

**LANDLORD ASSOCIATION OF PENNSYLVANIA**  
(LAPA)

**SUBSCRIBER SERVICE AGREEMENT**

---

Subscriber Service Agreement entered into as of \_\_\_\_\_ by Landlord Association  
(Date)

of Pennsylvania (LAPA) and \_\_\_\_\_

(“Subscriber”)

**SECTION ONE. Statement of LAPA and Subscriber Responsibilities:**

**LAPA Agrees:**

- 1.1 LAPA shall resell to Subscriber on request, credit information on consumers, businesses or corporations stored in LAPA computerized credit reporting system or obtained from other reliable sources available to same.
- 1.2 LAPA will exercise its best efforts to deliver credit or other information requested by Subscriber in an expeditious and efficient manner, but it shall have no obligation or liability to Subscriber for the accuracy, timeliness, completeness, merchantability or fitness for a particular purpose of the services, information in the services or the media on or through which the services are provided under this agreement.
- 1.3 LAPA shall respectively exercise its best efforts to furnish to Subscriber accurate and reliable information, but does not guarantee the correctness, currency or completeness of such information. Neither LAPA, nor its officers, employees, agents or suppliers shall be liable to Subscriber for any claim, injury or damage consequent upon furnishing such information.

**Subscriber Agrees:**

- 1.5 Subscriber shall provide LAPA with appropriate identifying information as to itself and the consumer when requesting information.
- 1.6 Subscriber hereby certifies and agrees that its operation is in compliance with Public Law 91-508 (Fair Credit Reporting Act) and all other applicable state and federal statutes and will request and use credit information received from LAPA solely in connection with transactions pursuant to the following terms:
- 1.7 Subscriber agrees to pay LAPA the applicable charge quoted by LAPA to Subscriber for the various services rendered to Subscriber. Payment by Subscriber shall be due ten (20) days following receipt of invoice. A late payment charge of 1½% per month will be imposed on overdue payments. Subscriber will be liable for all legal and other costs and expenses incurred by Subscriber Name, including but not limited to reasonable attorneys’ fees in the event that LAPA must take action to secure payment for services rendered to Subscriber.
- 1.8 Subscriber hereby certifies and agrees that it is responsible for the security of its Subscriber number and password assigned to this account and all usage resulting there from. Subscriber acknowledges that the services it receives from LAPA under this agreement include personal information on individual consumers and, as such, require confidential treatment.

**SECTION TWO Requests for Employment Reports:**

**Subscriber Agrees:**

- 2.1 Subscriber will provide a clear and conspicuous disclosure (in a document that consists solely of the disclosure) to the consumer indicating that a consumer report may be obtained for the purpose of employment and it will receive, in writing, the consumer’s consent to procure a consumer report.
- 2.2 Subscriber will adhere to all applicable federal or state equal employment opportunity laws or regulations with respect to information received from the consumer report.
- 2.3 Before taking any adverse action based on information obtained from the consumer report, Subscriber agrees to provide the consumer with a copy of the report and a written description of the consumer’s rights under the provisions of the Federal Trade Commission Section 609(c)(3).

**SECTION THREE. Covenants and Indemnification:**

- 3.1 LAPA shall indemnify, defend and hold Subscriber harmless from and against any and all costs and liabilities which may be asserted against Subscriber based upon improper use by LAPA of credit or other information furnished to LAPA by Subscriber. Subscriber shall indemnify, defend and hold LAPA harmless from and against any and all costs and liabilities which may be asserted against LAPA based upon the improper use by Subscriber of credit or other information furnished to Subscriber by LAPA.
- 3.2 This agreement shall continue in force without any fixed date of termination, but either LAPA or Subscriber may terminate the Agreement upon thirty days (30) prior notice to the other.
- 3.3 LAPA shall have no obligation or liability for or on the account of any mechanical or other breakdown, malfunction, or defect in computer or facilities or computer programs utilized by LAPA or Experian or any delay or failure in LAPA’s performance under this Agreement when such is beyond the reasonable control of LAPA. LAPA will use reasonable efforts to prevent such delay or failure and shall attempt to correct any such delay or failure as promptly as possible.
- 3.4 The warranties set forth in this Agreement apply to the performance of both parties hereunder, and are in lieu of all other warranties, expressed or implied, including without limitation, the warranties of merchantability and fitness for a particular purpose which are hereby disclaimed.

Subscriber's type of business: \_\_\_\_\_

Purpose for which the reports will be used: \_\_\_\_\_

In Witness Whereof. **LAPA** and Subscriber have caused this Agreement to be executed by their duly authorized representatives as of the date first above written.

Subscriber Name: \_\_\_\_\_

Subscriber Address: \_\_\_\_\_

\_\_\_\_\_

Contact Name: \_\_\_\_\_

Email Address: \_\_\_\_\_

Phone Number: \_\_\_\_\_

Fax Number: \_\_\_\_\_

By: \_\_\_\_\_

*(Authorized Signature)*

\_\_\_\_\_

*(Print Name and Title)*

---

**LANDLORD ASSOCIATION OF PENNSYLVANIA**

1414 Millard Street

Bethlehem, Pa 18018

(610) 867-8940 Fax (610) 867-8604

By: \_\_\_\_\_

*(Authorized Signature) (LAPA Only)*

\_\_\_\_\_

*(Print Name and Title) (LAPA Only)*



**The Landlord Association of Pennsylvania**

1414 Millard Street ▪ Bethlehem, Pa 18018

Tel. (610) 867-8904 ▪ Fax (610) 867-8604

## PERSONAL GUARANTEE AGREEMENT

I certify that I am the person named below. As principal of \_\_\_\_\_  
\_\_\_\_\_  
I authorize LAPA to review my credit  
profile to be used in conjunction with this application for company membership only  
and guarantee payment of any and all credit-reporting obligations to the company  
listed above.

**Name:** \_\_\_\_\_ **Social Security #** \_\_\_\_\_

**Home Address:**

---

---

**Previous Address:**

---

---

---

\_\_\_\_\_  
**Signature and Title**

## END USER AUTHORIZATION FORM (ONLINE ACCESS)

This form is to be used by Experian Reseller end user (End User) to identify the individual that will have access to Experian via the internet. The end user will submit all requests to create, change or lock End User access accounts and permissions to Experian systems and information via the Internet to the Experian Reseller Head Designate. End User(s) must be a duly appointed representative of the End User company and must be available to interact with Experian's Reseller on information and product access matters, in accordance with Experian Security Guidelines. Such Guidelines may be updated from time to time by Experian, and it is the responsibility of the End User to monitor the Guidelines for any updates. The Reseller End User Authorization Form must be signed by an authorized representative of the End User. End User acknowledges and agrees that they: 1) have received the Experian Security Guidelines, 2) have read and understands End User's obligations described in the Guidelines, 3) 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 4) will abide by the provisions of the Guidelines as well as the terms and conditions of the existing membership agreement(s). Changes in the End User status (e.g., transfer or termination) are to be reported to immediately to the Reseller Head Designate. **NOTE: Please see reverse for instructions on completing this form.**

End User INFORMATION (All fields are required unless stated)

<i>End User Status (Check One)</i>	<b>Create</b>	<input type="checkbox"/>	<b>Change</b>	<input type="checkbox"/>	<b>Lock</b>	<input type="checkbox"/>
<i>User ID (first choice)</i> [min. 6 chars.]						
<i>User ID (second choice)</i> [min. 6 chars.]						
<i>User ID (third choice)</i> [min. 6 chars.]						
<i>Add Co ID (optional)</i>						
<i>End User Company Name</i> (do not abbrev.)						
<i>Last Name</i>						
<i>First Name</i>						
<i>E-mail Address</i>						
<i>Telephone Number</i>						Ext.
<i>Product(s) Requested</i>						

Comments

### REPRESENTATIVE INFORMATION (Signature Required)

As an End User of Experian's products and services over the Internet, I am acting as the authorized representative of the End User. I hereby submit the above individual as an End User of my company and authorize Experian's Reseller to direct all Information Security related questions to same.

<i>Print Name</i>		<i>Title</i>	
<i>Signature</i>		<i>Date</i>	

### FOR RESELLER INTERNAL USE ONLY

(Do Not Write Below This Line)

<i>Date Sent/Faxed to Reseller</i>		<i>Reseller Group Preamble</i>	
<i>Reseller Security Designate (Requestor)</i>			
<i>Signature</i>		<i>Date</i>	



## Information Services

1414 Millard Street  
Bethlehem, Pa 18018  
Tel. (610) 867-5044 ▪ Fax (610) 867-8603

# 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. 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. Capitalized terms used herein have the meaning given in the Glossary attached hereto. 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:

## 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 system access software or is no longer used;
  - the hardware on which the software resides is upgraded, changed or disposed of
- 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 Ensure that user IDs are not shared and that no Peer-to-Peer file sharing is enabled on those users' profiles.
- 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 and letters)
  - Contain a minimum of seven (7) alpha/numeric characters for standard user accounts
- 1.9 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.
- 1.10 Active logins to credit information systems must be configured with a 30 minute inactive session, timeout.
- 1.11 Restrict the number of key personnel who have access to credit information.
- 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 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.
- 1.15 After normal business hours, turn off and lock all devices or systems used to obtain credit information.
- 1.16 Implement physical security controls to prevent unauthorized entry to your facility and access to systems used to obtain credit information.

## 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, 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 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.
  - On a weekly basis at a minimum, keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and installing new virus definition files.
- 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 on any laptop computer and in the database using AES or 3DES with 128-bit key encryption at a minimum.
- 3.5 Only open email attachments and links from trusted sources and after verifying legitimacy.

### **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 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.
- 4.3 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.
- 4.4 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security within your organization.

### **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 Encrypt Wireless access points with a minimum of WEP 128 bit encryption, WPA encryption where available.
- 5.6 Disable vendor default passwords, SSIDs and IP Addresses on Wireless access points and restrict authentication on the configuration of the access point.

## **6. Regularly Monitor and Test Networks**

- 6.1 Perform regular tests on information systems (port scanning, virus scanning, vulnerability scanning).
- 6.2 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 credit reporting agency 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.

**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, the credit reporting agency 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 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.*

*“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.”*

---

Signature/Title

---

Date

## Glossary Term

## Definition

<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 our 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 credit reporting agency account number.
<b>WEP Encryption</b>	(Wired Equivalent Privacy) A part of the wireless networking standard intended to provide secure communication. The longer the key used, the stronger the encryption will be. Older technology reaching its end of life.
<b>WPA</b>	(Wi-Fi Protected Access) A part of the wireless networking standard that provides stronger authentication and more secure communications. Replaces WEP. Uses dynamic key encryption verses static as in WEP (key is constantly changing and thus more difficult to break than WEP).



---

# **Experian Internet Security Guidelines**

**Version .9a**

**Standards Development**

**November 2001**

**Experian Private/Proprietary**

## Experian Internet Security Guidelines

### General

1. Experian fully supports and implements practices, which protect the confidential nature of the information in our databases and respects the consumers' right to privacy. Therefore, only companies that are approved members of our services ("Subscribers") and have permissible purpose for obtaining credit information and other reports are permitted to access the applications, which Experian provides to access this sensitive information.
2. To this end, it is important that all Subscribers take appropriate precautions to secure any systems (hardware and software) used to access Experian information systems, and ensure that all of the Subscriber's personnel who have been granted access to Experian information systems adhere to the Internet Security Guidelines provided herein.
3. These guidelines describe the general expectations and security requirements with respect to handling information, access to, and usage of Experian information systems by our Subscribers, and their Authorized Users. One of the purposes of these guidelines is to clarify the standards of behavior required of Subscribers and their employees who have been granted access to Experian information system assets. It is the responsibility of each authorized system user to ensure that all possible measures are taken to protect the confidential nature of the information that is provided and to protect the integrity of the systems providing this information.
4. As security threats and vulnerabilities along with the technologies and methods available to mitigate the resultant risks is an ever-changing landscape, these guidelines may periodically change to reflect this new environment.

### Guidelines

1. The Subscriber shall designate in writing, an employee to act as its Head Designate to act as the primary interface with Experian on systems access related issues. The Subscriber's Head Designate will be responsible for establishing, administering and monitoring all Subscriber's employee's internet access, or approving and establishing Security Designates to perform such functions.
2. The Subscriber's Head Designate or Security Designate shall in turn review all employee requests for Internet access approval. The Head Designate or its Security Designate shall determine the appropriate access to each Experian product based upon the legitimate business needs of each employee.
3. Unless automated means become available, the Subscriber shall request employee's (Internet) user access via the Head Designate/Security Designate in writing, in the format approved by Experian. Those employees approved by the Head Designate or Security Designate for internet access ("Authorized Users") will be individually assigned unique access identification numbers ("User ID") and passwords (this also applies to the unique Server-to-Server access IDs and passwords). 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 Subscriber), and reserves the right to change passwords and to revoke any authorizations previously granted. *Note: Partially completed forms and verbal requests will not be accepted.*
4. Only Authorized Users shall access Experian services (via the Internet), and only through the User ID and password assigned to such Authorized User by Experian or by the Head Designate or its Security Designate (as delegated and approved by Experian). Subscribers shall request User IDs and passwords only for those employees who have a legitimate need to access the services in performing his or her duties for the Subscriber. Prior to requesting User IDs for Authorized Users, Subscriber shall provide adequate training regarding these security procedures and any other applicable laws and regulations. Subscriber will ensure that each Authorized User is familiar with the requirements specified herein, and agrees to comply with such requirements, (ii) agrees not to disclose the User ID and password assigned to the Authorized Users to any other person, and (iii) agrees not to order credit reports or other data from Experian except in performance of employee's official duties for Subscriber.
5. Subscriber acknowledges and agrees that it is responsible for all activities of its employees/Authorized Users utilizing the Internet to access Experian services, and for assuring the facilities for receipt of information provided to it through the Internet are secure and in compliance with its membership agreement(s) covering such services. Subscriber shall not retransmit or otherwise make available to any person the services (including any of the information therein) on or through the Internet or other generally accessible network or delivery method.
6. Subscriber acknowledges and agrees that these guidelines and procedures are in addition to the procedures of the membership application process, including any access security requirements (except where expressly modified by these Experian Internet Security Guidelines). Subscriber will abide by any additional or further security procedures specified by Experian from time to time.
7. Subscriber shall use its best efforts to ensure the confidentiality of all User IDs and passwords issued. Subscriber shall indemnify Experian against any damage or disruption to Experian systems or business caused by its employees, subcontractors, subcontractor employees or its clients whether as a result of their access to such systems or compromise of password confidentiality or otherwise.
8. Subscriber understands that its use of Experian networking and computing resources may be monitored and audited by Experian, without further notice. Experian may from time to time audit the security mechanisms Subscriber maintains to

safeguard access to Experian information, systems and electronic communications. Audits may include examination of systems security and associated administrative practices.

9. In cases where the Subscriber is accessing Experian information and systems via Experian certified software, the Subscriber agrees to make available to Experian upon request, audit trail information and management reports generated by the vendor software, regarding Subscriber's individual Authorized Users.
10. Subscriber shall be responsible for and ensure that Experian certified vendor 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.

## Reporting

1. An officer of Subscriber's company agrees to notify Experian in writing immediately if it wishes to change or delete any employee as a Head Designate, Security Designate, or Authorized User; or if the identified Head Designate, Security Designate or Authorized User is terminated or otherwise loses his or her status as an Authorized User.
2. Audit trail reports (e.g. system access records, copies of Head Designate Authorization Form, etc.) shall be made available to Experian upon request.
3. Subscriber agrees to report to Experian's Information Security Office immediately, any compromise or suspected compromise of security, which may lead to a compromise or threat to Experian information systems.

## Roles and Responsibilities

### Head Designate

1. Subscriber agrees to identify an employee it has designated to act on its behalf as a primary interface with Experian on systems access related issues. This individual shall be identified as the "Head Designate." The Head Designate can further identify a Security Designate(s) to provide the day to day administration of the Authorized Users. Security Designate(s) must be a duly appointed representative of the Subscriber's company and shall be available to interact with Experian on information and product access, in accordance with these Experian Internet Security Guidelines. The (Head) Designate Authorization Form must be signed by a duly authorized representative of the Subscriber. Subscriber's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Subscriber Head Designate. The Head 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) Designate status (e.g. transfer or termination) are to be reported to Experian immediately.
2. As a Subscriber to Experian's products and services via the Internet, the Head Designate is acting as the duly authorized representative of Subscriber.
3. The Security Designate may be appointed by the Head Designate as the individual that Subscriber authorizes to act on behalf of the business in regards to Experian product access control (e.g. request to add/change/remove access). Subscriber can opt to appoint more than one Security Designate (e.g. for backup purposes). Subscriber understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaison with Experian's Security Administration group on information and product access matters.

### Security Designate

1. Must be a duly appointed representative of Subscriber's company, identified as an approval point for Subscriber's Authorized Users.
2. Is responsible for the initial and on-going authentication and validation of Subscriber's Authorized Users and must maintain current information about each (phone number, valid email address, etc.).
3. Must notify Experian to add, change, and lock users within Subscriber's company, if no automated facilities have been provided.
4. Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized User's job responsibilities.
5. Must ensure that standard security administration functions are performed within Subscriber's company. These include periodic review of Authorized User's activities, Authorized User's access rights, inactivity reviews, authentication and authorization process review, etc.
6. Is responsible for ensuring that Subscriber's Authorized Users are authorized to access Experian products and services.
7. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Subscriber.
8. Ensure password and ID records remain secure in Subscriber's environment and are issued to and shared only with the appropriate Authorized User.
9. Must advise Authorized Users not to share/post password or ID information.
10. Must advise Authorized Users of their responsibility to access consumer information for specified business uses only.

11. Must advise Authorized Users not to leave their workstations unattended when accessing Experian products and services.
12. Must advise Authorized Users to secure any Experian provided or generated documentation.
13. Must immediately report any suspicious or questionable activity to Experian regarding access to Experian's products and services.
14. Must report any potential compromise of Subscriber's systems that may expose Experian provided products or data to security threats.
15. Must communicate to Authorized Users, these security practices and regularly audit compliance, within Subscriber's organization.
16. Shall report changes in their Head Designate's status (e.g. transfer or termination) to Experian.
17. Will provide first level support for inquiries about passwords or IDs requested by your Authorized Users. Experian reserves the right to audit the processes employed and the documentation used to ensure Subscriber's Authorized User ID and password security. Any weakness or lack of documentation, as well as any User ID or password compromise may result in temporary suspension or termination of Subscriber's access rights.
18. Shall be available to interact with Experian when needed on matters of user access and authorization.

## Authorized Users

1. Shall use only the User ID and password which has been assigned to them. These User IDs and passwords are not to be shared and each Authorized User shall be held accountable for all actions, which occur under that User ID.
2. Shall immediately notify the Security Designate or Head Designate when the Experian product access is no longer required.
3. Shall protect their assigned User ID and password from unauthorized use.
4. Shall not exceed those permissions, which have been granted for system access.
5. Shall access consumer information for specified business uses only.

## Do's And Don'ts

### User IDs and Passwords

The following are just a few guidelines that should be considered by Authorized Users in constructing passwords:

1. Do **not** use your login name in any form (i.e. as is, reversed, caps, doubled...etc.).
2. Do **not** use your first, middle or last name in any form.
3. Do **not** use other information easily obtained about you (i.e. employee number, child or spouse's name, address...etc.).
4. Do **not** use a password of all digits, or all the same letters.
5. Do **not** use a word contained in English or foreign language dictionaries.
6. Do **not** use a password shorter than six characters.
7. **Do** use a password with mixed case alphabetic.
8. **Do** use a password that is easy to remember, so you don't have to write down.
9. **Do** change your password often enough to prevent an unauthorized person from guessing your password (every 90 days is suggested).
10. **Do** change your password **immediately** if you believe it has been compromised and notify the Head Designate, Security Designate, or Experian's Security Administration group.
11. **Do** change your password, the first time you log onto a new system.

### Other General Guidelines To Follow Include:

1. Do **not** share your password with anyone (Experian security administrators and Experian service desk personnel should not be asking you for your password).
  2. Do **not** share your user account or allow anyone to use your account while your workstation is unattended (log off or the use of password controlled screen savers can help reduce this risk).
  3. Do **not** write your password down and post it (or try to hide it) in an obvious location (i.e. don't post-it on your monitor, hide it in your desk calendar, under your desk pad or keyboard ... etc.).
  4. Do **not** repeat your passwords for at least 18 iterations.
  5. Do **not** use Experian systems to promote and exercise, unauthorized attempts to access Experian systems for which access has not been granted, or other non-Experian systems.
- Do** notify the Security Designate when the account is no longer needed.