ATLANTIC
Personnel & Tenant Screening, Inc.

# MEMBERSHIP APPLICATION

Company Name: _____

Doing Business As: _____

Contact Name: _____ Title: _____

Company Main Phone: _____ Answering Service ___ Yes ___No

Company Fax Number: _____ Email Address: _____

Company Website address: _____

Permissible Purpose (purpose you will utilize Atlantic's reports): _____

Physical Address: _____
Street City State County Zip

Billing Address (if different): _____
Street/PO City State County Zip

Number of Employees: _____

Nature of Business: _____ Date Established: _____

Is the applicant engaged in the underwriting of insurance? ___Yes __ No

Is the company licensed or providing service as an Attorney or detective/investigative agency:? ___Yes __No

If yes, indicate which: _____

Does the company intend to resell or release information from the consumer credit report to a third party: ___Yes __No

Will the company, or does the company provide credit repair or credit counseling services for a fee? ____Yes __No

**Complete for Sole Proprietor or Partnership (circle which):**

Owner Name: _____

Resident Address: _____
Street City State County Zip

Social Security #: _____ Signature: _____

Owner Name: _____

Resident Address: _____
Street City State County Zip

Social Security #: _____ Signature: _____

**8895 N. Military Trail #301C • Palm Beach Gardens, FL 33410**
**(561) 776-1804 (877) 747-2104 • Fax (561) 776-1565 (877) 747-2105**

ATLANTIC
Personnel & Tenant Screening, Inc.

# MEMBERSHIP APPLICATION

**Complete for Corporation:**

Officer Name: _____ Title: _____

Officer Name: _____ Title: _____

Officer Name: _____ Title: _____

Federal Tax ID #: _____

Bank Information:

Name of Bank: _____ Address: _____

Bank Phone Number: _____

Business Checking Account Information:

Name of Account: _____ Account Number: _____

Business References: (Provide three references)

1.) Business Name: _____ Business Phone: _____

Contact Name: _____

2.) Business Name: _____ Business Phone: _____

Contact Name: _____

3.) Business Name: _____ Business Phone: _____

Contact Name: _____

I certify that the information provided on this application is true.

Signature: _____ Date: _____

Print Name: _____ Title: _____

**8895 N. Military Trail #301C • Palm Beach Gardens, FL 33410**
**(561) 776-1804 (877) 747-2104 • Fax (561) 776-1565 (877) 747-2105**

ATLANTIC
Personnel & Tenant Screening, Inc.

# SERVICE AGREEMENT

1. Reseller has access to consumer reports from one or more consumer reporting agencies.
2. Subscriber is a _____ (type of business) and has a permissible purpose for obtaining consumer reports, as defined by Section 604 of the Federal Fair Credit Reporting Act (15 USC 1681b) as amended by the Consumer Credit Reporting Reform Act of 1996, hereinafter called "FCRA." The subscriber certifies their permissible purpose as:

   **In connection with tenant screening application involving the consumer**
3. Subscriber certifies that it will request consumer reports pursuant to procedures prescribed by Reseller from time to time only for the permissible purpose certified above, and will use the reports obtained for no other purpose.
4. Subscriber will maintain copies of all written authorizations for a minimum of five (5) years from the date of inquiry.
5. THE FCRA PROVIDES THAT ANY PERSON WHO KNOWINGLY AND WILLFULLY OBTAINS INFORMATION ON A CONSUMER FROM A CONSUMER REPORTING AGENCY UNDER FALSE PRETENSES SHALL BE FINED UNDER TITLE 18, OR IMPRISONED NOT MORE THAN TWO YEARS, OR BOTH.
6. Subscriber shall use each consumer report only for a one-time use and shall hold the report in strict confidence, and not to disclose it to any third parties; provided, however, that Subscriber may, but is not required to, disclose the report to the subject of the report only in connection with an adverse action based on the report. Moreover, unless explicitly authorized in this Agreement or in a separate agreement, between Reseller and Subscriber, for scores obtained from Trans Union LLC & Experian, or as explicitly otherwise authorized in advance and in writing by Trans Union LLC & Experian through Reseller, Subscriber shall not disclose to consumers or any third party, any nor all such scores provided under this Agreement, unless clearly required by law.
7. With just cause, such as delinquency or violation of the terms of this contract or a legal requirement, or a material change in existing legal requirements, which adversely affects this Agreement, Reseller may, upon its election, discontinue serving the Subscriber and cancel this Agreement immediately.

8. Subscriber agrees they WILL NOT resell any Atlantic Personnel & Tenant Screening report

_____
Company Name

Atlantic Personnel & Tenant Screening:

_____
Signature

_____
Signature

_____
Date

_____
Date

**8895 N. Military Trail #301C • Palm Beach Gardens, FL 33410**
**(561) 776-1804 (877) 747-2104 • Fax (561) 776-1565 (877) 747-2105**

ATLANTIC
Personnel & Tenant Screening, Inc.

**FCRA Requirements**

Federal Fair Credit Reporting Act (as amended by the
Consumer Credit Reporting Reform Act of 1996)

Although the FCRA primarily regulates the operations of consumer credit reporting agencies, it also affects you as a user of information. We have included a copy of the FCRA with your membership kit. We suggest that you and your employees become familiar with the following sections in particular:

§ 604. Permissible Purposes of Reports
§ 607. Compliance Procedures
§ 615. Requirement on users of consumer reports
§ 616. Civil liability for willful noncompliance
§ 617. Civil liability for negligent noncompliance
§ 619. Obtaining information under false pretenses
§ 621. Administrative Enforcement
§ 623. Responsibilities of Furnishers of Information to Consumer Reporting Agencies
§ 628. Disposal of Records

Each of these sections is of direct consequence to users who obtain reports on consumers.

As directed by the law, credit reports may be issued only if they are to be used for extending credit, review or collection of an account, employment purposes, underwriting insurance or in connection with some other legitimate business transaction such as in investment, partnership, etc. It is imperative that you identify each request for a report to be used for employment purposes when such report is ordered. Additional state laws may also impact your usage of reports for employment purposes.

We strongly endorse the letter and spirit of the Federal Fair Credit Reporting Act. We believe that this law and similar state laws recognize and preserve the delicate balance between the rights of the consumer and the legitimate needs of commerce.

In addition to the Federal Fair Credit Reporting Act, other federal and state laws addressing such topics as computer crime and unauthorized access to protected databases have also been enacted. As a prospective user of consumer reports, we expect that you and your staff will comply with all relevant federal statutes and the statutes and regulations of the states in which you operate.

We support consumer reporting legislation that will assure fair and
equitable treatment for all consumers and users of credit information.

_____ _____

Signature/Title Date

**Access Security Requirements for Reseller End-Users**
**for FCRA and GLB 5A Data**

**8895 N. Military Trail #301C • Palm Beach Gardens, FL 33410**
**(561) 776-1804 (877) 747-2104 • Fax (561) 776-1565 (877) 747-2105**

ATLANTIC
Personnel & Tenant Screening, Inc.

The following information security controls are required to reduce unauthorized access to consumer information. It is your (company provided access to Experian systems or data through Atlantic Personnel & Tenant Screening, Inc., referred to as the "Company") responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to get an outside service provider to assist you. Atlantic Personnel & Tenant Screening, Inc., 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 Atlantic Personnel & Tenant Screening, Inc., services, Company agrees to follow these Experian 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 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 Atlantic Personnel & Tenant Screening, Inc., will ever contact you and request your credentials.

1.2 If using third party or proprietary system to access Atlantic Personnel & Tenant Screening, Inc., 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 Atlantic Personnel & Tenant Screening, Inc., data/systems.

1.3 If the third party or third party software or proprietary system or software, used to access Atlantic Personnel & Tenant Screening, Inc., 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 Atlantic Personnel & Tenant Screening, Inc., 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) 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 (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 Company must NOT install Peer-to-Peer file sharing software on systems used to access, transmit or store Experian data.

1.14 Ensure that Company 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 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 (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 Experian data is classified 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 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 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 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 Experian data may have been compromised, immediately notify* Atlantic Personnel & Tenant Screening, Inc., *within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).*

4.4 The FACTA Disposal Rules requires that Company 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 Experian data, 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 Company's responsibility to ensure the service provider is engaged with Experian and an 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 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 Atlantic Personnel & Tenant Screening, Inc., 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 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 telecommunications systems and any computer system or network device(s) used to provide Services hereunder to access Atlantic Personnel & Tenant Screening, Inc., 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 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** Atlantic Personnel & Tenant Screening, Inc., 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 Atlantic Personnel & Tenant Screening, Inc., 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 Atlantic Personnel & Tenant Screening, Inc., 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 Atlantic Personnel & Tenant Screening, Inc., 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 Atlantic Personnel & Tenant Screening, Inc., systems shall be made available to Atlantic Personnel & Tenant

Screening, Inc., upon request, for example during breach investigation or while performing audits

**8.6** Data requests from Company to Atlantic Personnel & Tenant Screening, Inc., 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 Atlantic Personnel & Tenant Screening, Inc., within twenty-four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to Atlantic Personnel & Tenant Screening, Inc., 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 877-747-2104. Email notification will be sent to erodriguez@atlanticscreening.com or davdellas@atlanticscreening.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 Atlantic Personnel & Tenant Screening, Inc., 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 Atlantic Personnel & Tenant Screening, Inc., networking and computing resources may be monitored and audited by Atlantic Personnel & Tenant Screening, Inc., 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 Atlantic Personnel & Tenant Screening, Inc., 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 Atlantic Personnel & Tenant Screening, Inc.

*Record Retention: The Federal Equal Credit Opportunity 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 $3,500 per violation."*

---

**Internet Delivery Security Requirements**

In addition to the above, following requirements apply where Company and their employees or an authorized agent/s acting on behalf of the Company are provided access to Atlantic Personnel & Tenant Screening, Inc., provided services via Internet ("Internet Access").

**General requirements:**

1. The Company shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with Atlantic Personnel & Tenant Screening, Inc., on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to Atlantic Personnel & Tenant Screening, Inc., provided services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such functions.
2. The Company'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 Atlantic Personnel & Tenant Screening, Inc., product based upon the legitimate business needs of each employee. Atlantic Personnel & Tenant Screening, Inc., 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 Company shall request employee's (Internet) user access via the Head Security Designate/Security Designate in writing, in the format approved by Atlantic Personnel & Tenant Screening, Inc. 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). Atlantic Personnel & Tenant Screening, Inc., approval of requests for (Internet) access may be granted or withheld in its sole discretion. Atlantic Personnel & Tenant Screening, Inc., 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 Company), 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 Company agrees to notify Atlantic Personnel & Tenant Screening, Inc., 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. Company agrees to identify an employee it has designated to act on its behalf as a primary interface with Atlantic Personnel & Tenant Screening, Inc., 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

Company and shall be available to interact with Atlantic Personnel & Tenant Screening, Inc., on information and product access, in accordance with these Experian Access Security Requirements for Reseller End-Users. The Head Security Designate Authorization Form must be signed by a duly authorized representative of the Company. Company's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Company'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 Atlantic Personnel & Tenant Screening, Inc., systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to Atlantic Personnel & Tenant Screening, Inc., immediately.

2. As a Client to Atlantic Personnel & Tenant Screening, Inc., products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Company.
3. The Security Designate may be appointed by the Head Security Designate as the individual that the Company authorizes to act on behalf of the business in regards to Atlantic Personnel & Tenant Screening, Inc., product access control (e.g. request to add/change/remove access). The Company can opt to appoint more than one Security Designate (e.g. for backup purposes). The Company understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with Atlantic Personnel & Tenant Screening, Inc., Security Administration group on information and product access matters.
4. The Head Designate shall be responsible for notifying their corresponding Atlantic Personnel & Tenant Screening, Inc., 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 Company, identified as an approval point for Company's Authorized Users.
2. Is responsible for the initial and on-going authentication and validation of Company'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 Company's Authorized Users are authorized to access Atlantic Personnel & Tenant Screening, Inc., products and services.
5. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Company.

6. Must immediately report any suspicious or questionable activity to Atlantic Personnel & Tenant Screening, Inc., regarding access to Atlantic Personnel & Tenant Screening, Inc., products and services.
7. Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to Atlantic Personnel & Tenant Screening, Inc.
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 Atlantic Personnel & Tenant Screening, Inc., when needed on any system or user related matters.

**8895 N. Military Trail #301C • Palm Beach Gardens, FL 33410**
**(561) 776-1804 (877) 747-2104 • Fax (561) 776-1565 (877) 747-2105**

ATLANTIC
Personnel & Tenant Screening, Inc.

**Glossary**

| Term | Definition |
|---|---|
| **Computer Virus** | 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. |
| **Confidential** | Very sensitive information. Disclosure could adversely impact your company. |
| **Encryption** | Encryption is the process of obscuring information to make it unreadable without special knowledge. |
| **Firewall** | 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. |
| **Information Lifecycle** | (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. |
| **IP Address** | 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. |
| **Peer-to-Peer** | 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. |
| **Router** | 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. |
| **Spyware** | 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. |
| **Experian Independent Third Party Assessment Program** | The Experian Independent 3rd Party Assessment is an annual assessment of an Experian Reseller's ability to protect the information they purchase from Experian.<br>EI3PA℠ requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Experian.<br>EI3PA℠ also establishes quarterly scans of networks for vulnerabilities. |
| **ISO 27001 /27002** | IS 27001 is the specification for an ISMS, an 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. |
| **PCI DSS** | The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. |
| **SSAE 16 SOC 2, SOC3** | Statement on Standards for Attestation Engagements (SSAE) No. 1<br>SOC 2 Report on Controls Related to Security, Availability, Processing Integrity, Confidentiality, and Privacy.<br>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). |
| **FISMA** | 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. |
| **CAI / CCM** | Cloud Security Alliance Consensus Assessments Initiative (CAI) was launched to perform research, create tools and create industry partnerships to enable cloud computing assessments.<br>The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. |

_____ _____

Signature/Title Date



**8895 N. Military Trail #301C • Palm Beach Gardens, FL 33410**
**(561) 776-1804 (877) 747-2104 • Fax (561) 776-1565 (877) 747-2105**

**This Credit Scoring Services Agreement,** ("Agreement"), dated:_____, between _____ ("End User") and Atlantic Personnel & Tenant Screening_____ ("Provider")

WHEREAS, Provider is an authorized reseller of Experian Information Solutions, Inc. ("Experian"); and

WHEREAS, Experian and Fair, Isaac Corporation ("Fair, Isaac") offer the "Experian/Fair, Isaac Model", consisting of the application of a risk model developed by Experian and Fair, Isaac which employs a proprietary algorithm and which, when applied to credit information relating to individuals with whom the End User contemplates entering into a credit relationship will result in a numerical score (the "Score" and collectively, "Scores"); the purpose of the models being to rank said individuals in order of the risk of unsatisfactory payment.

NOW, THEREFORE, For good and valuable consideration and intending to be legally bound, End User and Provider hereby agree as follows:

**1. General Provisions**

**A. Subject of Agreement**. The subject of this Agreement is End User's purchase of Scores produced from the Experian/Fair, Isaac Model from Provider.

**B. Application.** This Agreement applies to all uses of the Experian/Fair, Isaac Model by End User during the term of this agreement.

**C. Term.** This agreement is open ended with no expiration date.

**2. Experian/Fair, Isaac Scores**

**A. Generally**. Upon request by End User during the Term, Provider will provide End User with the Scores.

**B. Time of Performance**. Ongoing unless either party violates the terms of agreement OR 30 days written notice by either party and/or the end user type of business changes.

**C. Warranty**. Provider warrants that the Scores are empirically derived and statistically sound predictors of consumer credit risk on the data from which they were developed when applied to the population for which they were developed. Provider further warrants that so long as it provides the Scores, the Scores will not contain or use any prohibited basis as defined by the federal Equal Credit Opportunity Act, 15 USC Section 1691 *et seq*. or Regulation B promulgated thereunder. THE FOREGOING WARRANTIES ARE THE ONLY WARRANTIES PROVIDER HAS GIVEN END USER WITH RESPECT TO THE SCORES, AND SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, PROVIDER MIGHT HAVE GIVEN END USER WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. End User's rights under the foregoing warranties are expressly conditioned upon End User's periodic revalidation of the Experian/Fair, Isaac Model in compliance with the requirements of Regulation B as it may be amended from time to time (12 CFR Section 202 *et seq*.).

**D. Release.** End User hereby releases and holds harmless Provider, Fair Isaac and/or Experian and their respective officers, directors, employees, agents, sister or affiliated companies, and any third-party contractors or suppliers of Provider, Fair, Isaac or Experian from liability for any damages, losses, costs or expenses, whether direct or indirect, suffered or incurred by End User resulting from any failure of the Scores to accurately predict that a United States consumer will repay their existing or future credit obligations satisfactorily.

**3. Fees**

No additional fees in addition to current prices negotiated with provider.

**4. Intellectual Property**

**A. No License**. Nothing contained in this Agreement shall be deemed to grant End User any license, sublicense, copyright interest, proprietary rights, or other claim against or interest in any computer programs utilized by Provider, Experian and/or Fair, Isaac or any third party involved in the delivery of the scoring services hereunder. End User acknowledges that the Experian/Fair, Isaac Model and its associated intellectual property rights in its output are the property of Fair, Isaac.

**B. End User Use Limitations**. By providing the Scores to End User pursuant to this Agreement, Provider grants to End User a limited license to use information contained in reports generated by the Experian/Fair, Isaac Model solely in its own business with no right to sublicense or otherwise sell or distribute said information to third parties. Before directing Provider to deliver Scores to any third party (as may be permitted by this Agreement), End User agrees to enter into a contract with such third party that (1) limits use of the Scores by the third party only to the use permitted to the End User, and (2) identifies Experian and Fair, Isaac as express third party beneficiaries of such contract.

**C. Proprietary Designations**. End User shall not use, or permit its employees, agents and subcontractors to use, the trademarks, service marks, logos, names, or any other proprietary designations of Provider, Experian or Fair, Isaac or their respective affiliates, whether registered or unregistered, without such party's prior written consent.

**5. Compliance and Confidentiality**

**A. Compliance with Law**. In performing this Agreement and in using information provided hereunder, End User will comply with all Federal, state, and local statutes, regulations, and rules applicable to consumer credit information and nondiscrimination in the extension of credit from time to time in effect during the Term. End User certifies that (1) it has a permissible purpose for obtaining the Scores in accordance with the federal Fair Credit Reporting Act, and any similar applicable state statute, (2) any use of the Scores for purposes of evaluating the credit risk associated with applicants, prospects or existing customers will be in a manner consistent with the provisions described in the Equal Credit Opportunity Act ("ECOA"), Regulation B, and/or the Fair Credit Reporting Act, and (3) the Scores will not be used for Adverse Action as defined by the Equal Credit Opportunity Act ("ECOA") or Regulation B, unless adverse action reason codes have been delivered to the End User along with the Scores.

**B. Confidentiality**. End User will maintain internal procedures to minimize the risk of unauthorized disclosure of information delivered hereunder. End User will take reasonable precautions to assure that such information will be held in strict confidence and disclosed only to those of its employees whose duties reasonably relate to the legitimate business purposes for which the information is requested or used and to no other person. Without limiting the generality of the foregoing, End User will take suitable precautions to prevent loss, compromise, or misuse of any tapes or other media containing consumer credit information while in the possession of End User and while in transport between the parties. End User certifies that it will not publicly disseminate any results of the validations or other reports derived from the Scores without each of Experian's and Fair, Isaac's express written permission.

**C. Proprietary Criteria**. Under no circumstances will End User attempt in any manner, directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by Experian and/or Fair, Isaac in performing the scoring services hereunder.

**D. Consumer Disclosure**. Notwithstanding any contrary provision of this Agreement, End User may disclose the Scores provided to End User under this Agreement (1) to credit applicants, when accompanied by the corresponding reason codes, in the context of

bona fide lending transactions and decisions only, and (2) as clearly required by law.

**6. Indemnification and Limitations**

**A. Indemnification of Provider, Experian and Fair, Isaac**. End User will indemnify, defend, and hold each of Provider, Experian and Fair, Isaac harmless from and against any and all liabilities, damages, losses, claims, costs, and expenses (including attorneys' fees) arising out of or resulting from any nonperformance by End User of any obligations to be performed by End User under this Agreement, *provided that* Experian/Fair, Isaac have given End User prompt notice of, and the opportunity and the authority (but not the duty) to defend or settle any such claim.

**B. Limitation of Liability.** NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, UNDER NO CIRCUMSTANCES WILL PROVIDER, EXPERIAN OR FAIR, ISAAC HAVE ANY OBLIGATION OR LIABILITY TO END USER FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES INCURRED BY END USER, REGARDLESS OF HOW SUCH DAMAGES ARISE AND OF WHETHER END USER EXCEED THE FEES PAID BY END USER PURSUANT TO THIS AGREEMENT OR NOT END USER WAS ADVISED SUCH DAMAGES MIGHT ARISE. IN NO EVENT
**C.** SHALL THE AGGREGATE LIABILITY OF PROVIDER, EXPERIAN OR FAIR, ISAAC TO DURING THE SIX MONTH PERIOD IMMEDIATELY PRECEDING THE DATE OF END USER'S CLAIM.

**7. Miscellaneous**

**A. Third Parties**. End User acknowledges that the Scores results from the joint efforts of
**B.** Experian and Fair, Isaac. End User further acknowledges that each Experian and Fair, Isaac have a proprietary interest in said Scores and agrees that either Experian or the Fair, Isaac may enforce those rights as required.

**C. Complete Agreement**. This Agreement sets forth the entire understanding of End User and Provider with respect to the subject matter hereof and supersedes all prior letters of intent, agreements, covenants, arrangements, communications, representations, or warranties, whether oral or written, by any officer, employee, or representative of either party relating thereto.

End User agrees to execute new agreements as necessary to remain in compliance.

**IN WITNESS WHEREOF**, End User and Provider have signed and delivered this Agreement.

Reseller: **Atlantic Personnel & Tenant Screening, Inc.** Customer:_____

Signed:_____ Signed: _____

Date:_____ Date:_____

**8895 N. Military Trail #301C • Palm Beach Gardens, FL 33410**
**(561) 776-1804 (877) 747-2104 • Fax (561) 776-1565 (877) 747-2105**

ATLANTIC
Personnel & Tenant Screening, Inc.

# END USER CERTIFICATION OF COMPLIANCE
## California Civil Code - Section 1785.14(a)

Section 1785.14(a), as amended, states that a consumer credit reporting agency does not have reasonable grounds for believing that a consumer credit report will only be used for a permissible purpose unless all of the following requirements are met:

Section 1785.14(a)(1) states: "If a prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the consumer credit reporting agency shall, with a reasonable degree of certainty, match at least three categories of identifying information within the file maintained by the consumer credit reporting agency on the consumer with the information provided to the consumer credit reporting agency by the retail seller. The categories of identifying information may include, but are not limited to, first and last name, month and date of birth, driver's license number, place of employment, current residence address, previous residence address, or social security number. The categories of information shall not include mother's maiden name."

Section 1785.14(a)(2) states: "If the prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the retail seller must certify, in writing, to the consumer credit reporting agency that it instructs its employees and agents to inspect a photo identification of the consumer at the time the application was submitted in person. This paragraph does not apply to an application for credit submitted by mail."

Section 1785.14(a)(3) states: "If the prospective user intends to extend credit by mail pursuant to a solicitation by mail, the extension of credit shall be mailed to the same address as on the solicitation unless the prospective user verifies any address change by, among other methods, contacting the person to whom the extension of credit will be mailed."

In compliance with Section 1785.14(a) of the California Civil Code, _____ ("End User") hereby certifies to Consumer Reporting Agency as follows: (Please circle)

End User **(IS)** **(IS NOT)** a retail seller, as defined in Section 1802.3 of the California Civil Code ("Retail Seller") and issues credit to consumers who appear in person on the basis of applications for credit submitted in person ("Point of Sale").

End User also certifies that if End User is a Retail Seller who conducts Point of Sale transactions, End User will, beginning on or before July 1, 1998, instruct its employees and agents to inspect a photo identification of the consumer at the time an application is submitted in person.

End User also certifies that it will only use the appropriate End User code number designated by Consumer Reporting Agency for accessing consumer reports for California Point of Sale transactions conducted by Retail Seller.

If End User is not a Retail Seller who issues credit in Point of Sale transactions, End User agrees that if it, at any time hereafter, becomes a Retail Seller who extends credit in Point of Sale transactions, End User shall provide written notice of such to Consumer Reporting Agency prior to using credit reports with Point of Sale transactions as a Retail Seller, and shall comply with the requirements of a Retail Seller conducting Point of Sale transactions, as provided in this certification.

_____
End User

By:_____

Title:_____ Date: _____

**8895 N. Military Trail #301C • Palm Beach Gardens, FL 33410**
**(561) 776-1804 (877) 747-2104 • Fax (561) 776-1565 (877) 747-2105**

ATLANTIC
Personnel & Tenant Screening, Inc.

Dear Customer,

In an effort to cooperate with credit reporting compliance responsibilities under the Fair Credit Reporting Act, please list **all properties, contact name, property address, and property phone number** currently under your management and sign at the bottom.

Thank you for your attention in this matter.

The Staff,
Atlantic Personnel & Tenant Screening

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____ _____
Signature/Title Date

**8895 N. Military Trail #301C • Palm Beach Gardens, FL 33410**
**(561) 776-1804 (877) 747-2104 • Fax (561) 776-1565 (877) 747-2105**

ATLANTIC
Personnel & Tenant Screening, Inc.

# ADDENDUM TO SERVICE AGREEMENT

THIS ADDENDUM TO SERVICE AGREEMENT ("Agreement") is made and entered into by and between Atlantic Personnel & Tenant Screening, Inc. and _____ ("Subscriber"). This Agreement shall be effective on the date of the last signature below (the "Effective Date").

## Preamble

Atlantic Personnel & Tenant Screening, Inc. strives to deliver accurate and timely information products to assist your company (hereinafter "Subscriber") in making intelligent and informed decisions for a permissible purpose under applicable law. To this end, Atlantic Personnel & Tenant Screening, Inc. assembles information from a variety of sources, including databases maintained by consumer reporting agencies containing information from public records, other information repositories, and third-party researchers. Subscriber understands that these information sources and resources are not maintained by Atlantic Personnel & Tenant Screening, Inc. Therefore, Atlantic Personnel & Tenant Screening, Inc. cannot be a guarantor that the information provided from these sources is absolutely accurate or current. Nevertheless, Atlantic Personnel & Tenant Screening, Inc. has in place procedures designed to respond promptly to claims of incorrect or inaccurate information in accordance with applicable law.

## Subscriber's Re-Certification of Fair Credit Reporting Act (FCRA) Permissible Purpose(s)

Subscriber hereby certifies that all of its orders for information products from Atlantic Personnel & Tenant Screening, Inc. shall be made, and the resulting reports shall be used, for the following Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.,* permissible purposes only: *(Please check all that apply)*

| | |
|---|---|
| | Section 604(a)(2). As instructed by the consumer in writing. (Tenant Screening) |
| | Section 604(a)(3)(B). For employment purposes, including evaluating a consumer for employment, promotion, reassignment or retention as an employee, where the consumer has given prior written permission. |

**Subscriber's Re-Certification of Legal Compliance**

Subscriber certifies to Atlantic Personnel & Tenant Screening, Inc. that the information products it receives will not be used in violation of any applicable federal, state or local laws. Subscriber accepts full responsibility for complying with all such laws and for using the information products it receives from Atlantic Personnel & Tenant Screening, Inc. in a legally acceptable fashion. Subscriber further accepts full responsibility for any and all consequences of use and/or dissemination of those products.

Subscriber agrees to have reasonable procedures to secure the confidentiality of private information. Subscriber agrees to take precautionary measures to protect the security and dissemination of this information including, without limitation, restricting terminal access, utilizing passwords to restrict access to terminal devices, and securing access to, dissemination, and destruction of electronic and hard copy reports.

Likewise, as a condition of entering into this Agreement, Subscriber certifies that it has in place reasonable procedures designed to comply with all applicable local, state, and federal laws. Subscriber also certifies that it will retain any information it receives from Atlantic Personnel & Tenant Screening, Inc. for a period of five years from the date the report was received.

A. When Information Products are Used for Employment Purposes

If the information products Subscriber obtains from Atlantic Personnel & Tenant Screening, Inc. are to be used for an employment purpose, Subscriber certifies that prior to obtaining or causing a "consumer report" and/or "investigative consumer report" to be obtained, a clear and conspicuous disclosure, in a document consisting *solely of the disclosure*, will be made in writing to the consumer explaining that a consumer report and/or investigative consumer report may be obtained for employment purposes. This disclosure will satisfy all requirements identified in Section 606(a)(1) of the FCRA, as well as any applicable state or local laws. The consumer will have authorized, in writing, the obtaining of the report by Subscriber.

If the consumer may be denied employment or receive another adverse action based in whole or part on information products provided by Atlantic Personnel & Tenant Screening, Inc., Subscriber will provide to the consumer: (1) a copy of the report, and (2) a description, in writing, of the rights of the consumer entitled "A Summary of Your Rights Under the Fair Credit Reporting Act." After the appropriate waiting period, Subscriber will issue to the consumer notice of the adverse action taken, including the statutorily-required notice identified in Section 615 of the Fair Credit Reporting Act. Among other things, such notice will include: (1) the name, address, and telephone number of consumer reporting agency Atlantic Personnel & Tenant Screening, Inc, (2) a statement that the consumer reporting agency did not make the decision to take the adverse action and is unable to provide the consumer the specific reasons why the adverse action was taken, (3) a statement that the consumer may obtain a free copy of the consumer report from the consumer reporting agency within 60 days pursuant to Section 612 of the Fair Credit Reporting Act, and (4) a statement that the consumer has the right to dispute with the consumer reporting agency the accuracy or completeness of any information in a consumer report furnished by the agency.

Subscriber hereby acknowledges that it has received a copy of the Summary of Rights (16 C.F.R. Part 601, Appendix A) and Notice of Users of Consumer Reports (16 C.F.R. Part 601, Appendix C).

Subscriber also acknowledges that it is aware that local, state, and federal laws and regulations impact how and under what circumstances Subscriber may use criminal history information, credit history information, and other consumer report information. Subscriber assumes full responsibility for complying with all applicable laws and regulations. Among other things, Subscriber has or will become familiar with April 2012 EEOC Enforcement Guidance explaining how employers may utilize criminal history information in compliance with Title VII of the Civil Right Acts of 1964, as amended.

B. When Information Products Are Used For Tenant Screening Purposes

If the information products Subscriber obtains from Atlantic Personnel & Tenant Screening, Inc. are to be used for tenant screening, Subscriber agrees that it will first obtain the written consent of the consumer to do so.

If Subscriber takes adverse action against a tenant or prospective tenant based upon a consumer report or investigative consumer report from Atlantic Personnel & Tenant Screening, Inc., Subscriber agrees to follow all adverse action requirements specified in Section 615 of the Fair Credit Reporting Act. Among other things, Subscriber agrees that it will provide a notice to the consumer that includes: (1) the name, address, and telephone number of consumer reporting agency Atlantic Personnel & Tenant Screening, Inc., (2) a statement that the consumer reporting agency did not make the decision to take the adverse action and is unable to provide the consumer the specific reasons why the adverse action was taken, (3) a statement that the consumer may obtain a free copy of the consumer report from the consumer reporting agency within 60 days pursuant to Section 612 of the Fair Credit Reporting Act, and (4) a statement that the consumer has the right to dispute with the consumer reporting agency the accuracy or completeness of any information in a consumer report furnished by the agency.

**Additional Requirements for Investigative Consumer Reports**

In addition to the requirements identified above, and regardless of whether the screening is being done in connection with an employment or tenant situation, if the consumer makes a written request within a reasonable amount of time, Subscriber will provide: (1) information about whether an investigative consumer report has been requested; (2) if an investigative consumer report has been requested, written disclosure of the nature and scope of the investigation requested; and (3) Atlantic Personnel & Tenant Screening, Inc.'s contact information, including complete address and toll-free telephone number. This information will be provided to the consumer no later than five (5) days after the request for such disclosure is received from the consumer or such report is first requested, whichever is the latter.

**Additional Requirements for Motor Vehicle Records (MVRs) and Driving Records**

Subscriber hereby certifies that Motor Vehicle Records and/or Driving Records (MVRs) shall only be ordered in strict compliance with the Driver Privacy Protection Act ("DPPA" at 18 U.S.C. § 2721 *et seq.*) and any related state laws. Subscriber further certifies that no MVRs shall be ordered without first obtaining the written consent of the consumer to obtain "driving records," evidence of which shall be

transmitted to Atlantic Personnel & Tenant Screening, Inc. in the form of the consumer's signed release authorization form. Subscriber also certifies that it will use this information only in the normal course of business to obtain lawful information relating to the holder of a commercial driver's license or to verify information provided by an applicant or employee. Subscriber shall not transmit any data contained in the resulting MVR via the public internet, electronic mail or any other unsecured means.

**Additional Requirements for International Background Checks**

Subscriber understands that international background checks will be conducted through a third-party contractor. Because of differences in foreign laws, language, and the manner in which foreign records are maintained and reported, Atlantic Personnel & Tenant Screening, Inc. cannot be a guarantor or insurer of the accuracy of the information reported. Subscriber agrees to release Atlantic Personnel & Tenant Screening, Inc. and its affiliated companies, officers, agents, employees, and independent contractors, from any liability whatsoever in connection with international background checks performed by Atlantic Personnel & Tenant Screening, Inc.

**General Provisions**

Subscriber agrees not to resell, sub-license, deliver, display or otherwise distribute to any third party any of the information products addressed herein, except as required by law. Subscriber may not assign or transfer this Agreement without the prior written consent of Atlantic Personnel & Tenant Screening, Inc. If any of the provisions of this Agreement become invalid, illegal or unenforceable in any respect, the validity, legality, and enforceability of the remaining provisions shall not in any way be impacted. By agreement of the parties, Florida law shall guide the interpretation of this Agreement, if such interpretation is required. All litigation arising out of this Agreement shall be commenced in Florida**,** and the parties hereby consent to such jurisdiction and venue. Any written notice by either party shall be delivered personally by messenger, private mail courier service, or sent by registered or certified mail, return receipt requested, postage prepaid to the addresses listed below. This Agreement shall be construed as if it were jointly prepared. Both parties agree that this Agreement constitutes all conditions of service, present and future. Changes to these conditions may be made only by mutual written consent of an authorized representative of Subscriber and an officer of Atlantic Personnel & Tenant Screening, Inc. The headings of each section shall have no effect upon the construction or interpretation of any part of this Agreement.

If Subscriber is permitted to request consumer reports via Atlantic Personnel & Tenant Screening, Inc.'s website, then, in addition to all other obligations, Subscriber agrees to abide by such additional conditions that may be imposed to utilize the website, provide all required certifications electronically, to maintain complete and accurate files containing all required consent, authorization, and disclosure forms with regard to each consumer for whom a report has been requested, and maintain strict security procedures and controls to assure that its personnel are not able to use Subscriber's Internet access to obtain reports for improper, illegal or unauthorized purposes.

Subscriber agrees to allow Atlantic Personnel & Tenant Screening, Inc. to audit its records at any time, upon reasonable notice given. Breaches of this Agreement and/or violations of applicable law

discovered by Atlantic Personnel & Tenant Screening, Inc. may result in immediate suspension and/or termination of the account, legal action, and/or referral to federal or state regulatory agencies.

If there is a conflict between any of the terms of this Agreement and any terms of any other agreements between the Parties, the terms of this Agreement shall govern.

## Confidentiality

Neither party shall reveal, publish or otherwise disclose any Confidential Information to any third party without the prior written consent of the other party. "Confidential Information" means any and all proprietary or secret data; sales or pricing information relating to either party, its operations, employees, products or services, and all information relating to any customer, potential customer, Agent, and/or independent sales outlet. The Parties agree to keep this information confidential at all times during the term of this Agreement, and continuing for five years after receipt of any Confidential Information.

At all times during the term of this Agreement and after termination of this Agreement (regardless of the reason for termination), the Subscriber shall at all times keep secret and confidential all Atlantic Personnel & Tenant Screening, Inc. trade secrets which the Subscriber has acquired before or during the term of this Agreement and shall not disclose the trade secrets to any person or entity or directly or indirectly use the trade secrets for the Subscriber's own advantage without the prior written consent of Atlantic Personnel & Tenant Screening, Inc. Trade secrets shall have the definition provided for in Section 688.002(4) of the Florida Statutes.

Notwithstanding anything to the contrary herein, in no event shall Atlantic Personnel & Tenant Screening, Inc. be required to destroy, erase or return any consumer reports or applicant data related thereto in Atlantic Personnel & Tenant Screening, Inc.'s files, all of which Atlantic Personnel & Tenant Screening, Inc. shall maintain as a consumer reporting agency in strict accordance with all applicable federal, state, and local laws.

## Independent Contractor

The parties agree that the relationship of the parties created by this Agreement is that of independent contractor and not that of employer/employee, principal/agent, partnership, joint venture or representative of the other. Except as authorized hereunder, neither party shall represent to third parties that it is the employer, employee, principal, agent, joint venture or partner with, or representative of the other party.

## Fees and Payment

Subscriber agrees to pay nonrefundable fees and other charges or costs for Atlantic Personnel & Tenant Screening, Inc.'s employment screening services. Any charges or costs, including but not limited to surcharges and other fees levied by federal, state, county, other governmental agencies, educational institutions, employer verification lines and licensing agencies, incurred by Atlantic Personnel & Tenant Screening, Inc. in servicing Subscriber, will be passed on to Subscriber. At Atlantic Personnel & Tenant Screening, Inc.'s option, payments not received thirty (30) days after the date of the invoice may

cause the account to be placed on temporary interruption, with no additional requests being processed until the balance due is paid in full or arrangements have been made with Atlantic Personnel & Tenant Screening, Inc. Accounts with invoices unpaid thirty (30) days or more will be assessed an interest charge of 1-½% per month, as allowed by applicable law. If the account goes to collection, Subscriber agrees to pay all collection expenses, including attorneys' fees and court costs. Subscriber agrees that providing credit card information and submitting it electronically to Atlantic Personnel & Tenant Screening, Inc. presents a legal authorization to debit the card for the orders placed or for non-payment per the 15-day terms. Subscriber agrees that prices for services are subject to change without notice, although Atlantic Personnel & Tenant Screening, Inc. will make every reasonable effort to give notice of such change before it becomes effective. Any account that remains inactive for a period of twelve (12) months will be deemed inactive and may be terminated by Atlantic Personnel & Tenant Screening, Inc.

## Warranties and Remedies

Subscriber understands that Atlantic Personnel & Tenant Screening, Inc. obtains the information reported in its information products from various third party sources "AS IS" and, therefore, is providing the information to Subscriber "AS IS". Atlantic Personnel & Tenant Screening, Inc. makes no representation or warranty whatsoever, express or implied, including but not limited to, implied warranties of merchantability or fitness for particular purpose or implied warranties arising from the course of dealing or a course of performance with respect to the accuracy, validity or completeness of any information products and/or consumer reports, that the information products will meet Subscriber's needs or will be provided on an uninterrupted basis; Atlantic Personnel & Tenant Screening, Inc. expressly disclaims any and all such representations and warranties.

Subscriber agrees to indemnify, defend, and hold harmless Atlantic Personnel & Tenant Screening, Inc., its successors and assigns, officers, directors, employees, agents, vendors, and suppliers from any and all claims, actions or liabilities arising from or with respect to: (i) any breach by Subscriber of this Agreement or the representations, certifications or warranties made hereunder, (ii) Subscriber's violation of applicable laws or ordinances, (iii) Subscriber's negligence, misconduct, recklessness, errors or omissions, (iv) Subscriber's acquisition of or use of Atlantic Personnel & Tenant Screening, Inc.'s information products or services, or (v) Atlantic Personnel & Tenant Screening, Inc.'s preparation of or delivery of information products or services to Subscriber.

Atlantic Personnel & Tenant Screening, Inc. will not be liable for any indirect, incidental, consequential, or special damages for loss of profits, whether incurred as a result of negligence or otherwise, even if Atlantic Personnel & Tenant Screening, Inc. has been advised of the possibility of such damages.

Atlantic Personnel & Tenant Screening, Inc. does not guarantee Subscriber's compliance with all applicable laws in its use of reported information and does not provide legal or other compliance-related services upon which Subscriber may rely. Subscriber understands that Atlantic Personnel & Tenant Screening, Inc. is not a law firm and that any documents, communications or information received from Atlantic Personnel & Tenant Screening, Inc. regarding the obtainment or use of background screening reports is not to be considered legal counsel or legal opinion. Subscriber agrees that it will consult with its own legal or other counsel regarding the acquisition and use of background screening information,

including but not limited to, the legality of using or relying on reported information and the appropriate procedure for taking adverse action against an applicant based upon a consumer report.

**Term and Termination**

Either party may cancel this Agreement at any time. Termination of this Agreement by either party does not release Subscriber from its obligation to pay for services rendered or other responsibilities and agreements made.

**Force Majeure**

Subscriber agrees that Atlantic Personnel & Tenant Screening, Inc. is not responsible for any events or circumstances beyond its control (*e.g.*, including but not limited to war, riots, embargoes, strikes, and/or Acts of God) that prevent Atlantic Personnel & Tenant Screening, Inc. from meeting its obligations under this Agreement.

**Waiver**

The failure of either party to insist in any one or more cases upon the strict performance of any term, covenant or condition of this Agreement will not be construed as a waiver of subsequent breach of the same or any other covenant, term or condition; nor shall any delay or omission by either party to seek a remedy for any breach of this Agreement be deemed a waiver by either party of its remedies or rights with respect to such a breach.

**Severability**

If any provision of this Agreement, or the application thereof to any person or circumstance, shall be held invalid or unenforceable under any applicable law, such invalidity or unenforceability shall not affect any other provision of this Agreement that can be given effect without the invalid or unenforceable provision or the application of such provision to other persons or circumstances and, to this end, the provisions hereof are severable.

**Execution**

This Agreement may be executed in any number of counterparts, each of which shall be deemed an original, but all of which taken together shall constitute one and the same instrument. A signature on a copy of this Agreement received by either party by facsimile is binding upon the other party as an original. The parties shall treat a photocopy of such facsimile as a duplicate original. The individuals signing below represent that they are duly authorized to do so.

_____ _____
Company or Business Legal Name Date

_____
By (Signature of Authorized Officer Only)

_____
Printed Name

_____
Title

_____
Address

_____
Address

_____ / _____
Telephone Fax

_____
Email

_____
Company Website

**Default Subscriber Preferences**

Please return results via
Fax
Website

**Please sign and fax completed Subscriber Agreement to (561) 776-1565, Attn Erin .**

_____ _____
Approved by Date of Approval

_____
Printed Name

_____
Title

_____

_____
Address

**8895 N. Military Trail #301C • Palm Beach Gardens, FL 33410**
**(561) 776-1804 (877) 747-2104 • Fax (561) 776-1565 (877) 747-2105**