Credit Bureau
Phone 512 285-6078 Fax 512 285-6336
www.accuratecredit.com

Welcome to Accurate Credit Bureau

Accurate Credit Bureau provides Employers and Businesses with credit reporting, employee screening, and background checks. We also provide Judgment/collection companies, Landlords, Property managers, and Real Estate Agents with comprehensive credit reporting and tenant screening nationwide. To request background checks please complete the following.

[x] The Client Application filled out by you
[x] A copy of your ID (i.e. a drivers license, passport, or military ID)
[x] A letter of intent (Please describe the nature of your business and your intent for obtaining credit reports)
[x] A signed copy of the enclosed access security agreement
[x] A signed copy of the employment addendum
[x] A copy of a voided business check
[x] Copies of two utility bills (one bill from 2 different utilities)
[x] A copy of Business License

NOTE: We cannot accept PO Box addresses.

This information is only needed once to complete your file. It will allow us to instantly assign you an Accurate Client ID number. You may use your Client ID number to access our services instantly in the future without further documentation. There are no set up fees or membership required. **A copy of your prospective employee's Drivers License is mandatory.**

Looking forward to working with you.
Accurate Credit Bureau
Email: corp@accuratecredit.com

Accurate
Credit Bureau
Phone 512 285-6078 Fax 512 285-6336
www.accuratecredit.com

EMPLOYER CLIENT APPLICATION

We cannot accept PO Boxes

Name_____Date_____/_____/_____

Firm Name (If Applicable)_____Type of Business_____

Address_____City_____State_____Zip_____

E-mail Address_____

Home Phone #_____Day #_____Fax #_____

(Please Complete One of the Following) **Social Security** # _____or

Drivers License #_____or Federal Tax ID #_____

I will be ordering credit reports for [ ] Tenant Screening [ ] Employee Screening [ ] Line of Credit [ ] Judgment/Collections

Location Type is [ ] Commercial [ ] Residential

[ ] Yes, I would like to receive updates and product info from you in the future.

Credit Card you wish Billed? [ ] Visa [ ] MasterCard [ ] Discover [ ] Amex

Name of Cardholder_____

Credit Card #_____Expiration Date_____

I agree to comply and abide with the Fair Credit Reporting Act in its entirety. I also agree to the terms of the (included) Security Access Requirements Agreement. I agree to obtain an executed application from each applicant stating consent to view their consumer credit report and will keep the executed application confidentially on file for at least three years. I will not disclose any such information to any other party or resell any information provided to me by Accurate Credit Bureau.

Accurate
Credit Bureau
Phone 512 285-6078 Fax 512 285-6336
www.accuratecredit.com

Signature_____Date_____/_____/_____

ACCESS SECURITY REQUIREMENTS SERVICE AGREEMENT

We must work together to protect the privacy and information of consumers. The following information security measures are designed to reduce unauthorized access of 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 another system access software of 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 computer (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.

Accurate
Credit Bureau
Phone 512 285-6078 Fax 512 285-6336
www.accuratecredit.com

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 IO 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 Credit 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

Accurate
Credit Bureau
Phone 512 285-6078 Fax 512 285-6336
www.accuratecredit.com

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_____ Date_____

Print Name_____

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.
SSID	Part of the Wi-Fi Wireless LAN, a service set identifier (SSID) is a code that identifies each packet as part

Accurate
Credit Bureau
Phone 512 285-6078 Fax 512 285-6336
www.accuratecredit.com

	of that network. Wireless devices that communicate with each other share the same SSID.
Subscriber Code	Your seven digit credit reporting agency account number.
WEP Encryption	(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.
WPA	(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).

EMPLOYMENT ADDENDUM

Thank you for choosing Accurate Credit Bureau. In order to receive credit reports for employment purposes, you must first agree to the following addendum and will
ensure that prior to procurement or causing the procurement of a consumer credit report for employment purposes (an Employment Insight Report) that:

(1) a clear and conspicuous disclosure has been made in writing to the consumer at any time before the report is procured or caused to be procured, in a document that consists solely of the disclosure, that a consumer report be obtained for employment purposes; and
(2) the consumer has authorized in writing the procurement of the report and **provided a valid picture ID which must be sent to Accurate Credit Bureau**.

In using a consumer credit report for employment purposes, before taking any adverse action based in whole or in part on the report, the Subscriber shall provide to the consumer whom the report relates:

(1) a copy of the report
(2) a description in writing of the rights of the consumer under the Act, a copy of which is attached hereto ("Summary of Consumer Rights").

In addition, the information from the consumer report will not be used in violation of any applicable federal or state equal employment opportunity law or regulation.

Signature_____ Date_____

Print Name_____

Accurate

Credit Bureau

Phone 512 285-6078 Fax 512 285-6336

www.accuratecredit.com