SafestHires, Inc.

Policy: Information Security Certification Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as "the company".

Overview

It is important to maintain a current information security certification and/or to provide evidence of completing an information security audit for which no critical, high risk or severe security vulnerabilities remain uncured. Such certifications and/or written evidence must be completed by a qualified security assessor.

Purpose

To ensure the effectiveness of an information security program, it is important the applicable platform/data center hold a current security certification or demonstration that no severe security vulnerabilities remain uncured.

Scope

The scope of this policy includes all employees.

Policy

In all locations where PII (Personally Identifiable Information) or sensitive consumer information is held a current information security certification or evidence through a security audit that no critical, high risk, or severe security vulnerabilities remain uncured is be maintained. The source of such certification and/or written evidence is a qualified security assessor. Company maintains such documentation on file and ensures it is current at all times.

SafestHires, Inc.

Policy: Data Security Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

It is essential to follow a written information security program which at a minimum complies with applicable law and regulation. The program must designate one individual for the overall responsibility of the program to include implementing, managing, and enforcing the program.

Purpose

To avoid unnecessary risk, it is important that a formal informal information security program be maintained which at a minimum complies with applicable law. The program must designate one individual to maintain implementation, management, and enforcement authority.

Scope

The scope of this policy includes all employees.

Policy

The company has designated Andrew Andersen the individual responsible for implementation, management, and enforcement of its information security program.

The company has developed and maintains policies and procedures to ensure information security over broad areas within our environment. The policies and procedures detail the following elements to the overall information security program:

- Key Personnel, roles, and responsibilities
- Policy Changes and Modifications
- System Configuration
- Anti-Virus, firewall and router configuration
- Data and information classification
- Encryption
- Access Control
- Electronic Data Retention, Storage and Disposal
- Paper and hard data retention, storage, and Disposal
- Data Device retention, storage, and Disposal
- Incident Response
- Physical Security, and
- Security Policy Revision History

Key Personnel, Roles and Responsibilities

Andrew Andersen is responsible for the company overall information security program. He understands the critical nature of this responsibility and its importance to consumers, customers, and the company. He has the responsibility to implement, manage and enforce the information security program. He also has the responsibility and authority to call on other resources, both internal and external while performing these activities on behalf of the company.

Policy Changes, Modifications and Security Policy Revision History

Andrew Andersen is responsible for implementing, managing, and enforcing information security policy changes, modifications, and documenting revision history. This is a controlled document, and the company has policies and procedures to control document versions to ensure only the most updated version is applied internally and made available externally. Revisions to this policy are tracked.

System Configuration (Anti-virus, firewall, router, encryption, classification)

An information security certification is on file with the company for all locations that hold PII/Sensitive Consumer Information. The certificate is evidence of an information security audit by a qualified security assessor for which no critical, high-risk, or severe security vulnerabilities remain uncured. The company evidence includes the name of the security standard used as the basis for auditing and at least one of the following from a quality assessor:

1. Certification Document
2. Audit Results signed by a auditor showing no remaining uncured critical, high-risk, or severe security vulnerabilities, or
3. Signed attestation including date of audit, name of auditor(s), name of auditing company, and a statement that no critical, high-risk, or severe security vulnerabilities were found, or if found, such vulnerabilities have been cured.

The company configuration including anti-virus, firewall, router, and encryption along with the certification are outlined in our Certification Policy and all records are maintained.

Access Control

The company controls access to consumer information. Company access protocols may include:

1. Strong Passwords
2. Biometric Identification
3. Multifactor Authentication

Electronic/Paper/Hard Data and Device Retention, Storage, and Disposal

The company follows procedures to protect consumer information under our control from internal and external unauthorized access. These procedures include specifications for the securing of information when electronically transmitted, as well as information in both hard copy and electronic form including information stored on portable and/or removable electronic devices. These procedures meet all

applicable legal and regulatory requirements.

The company record retention and destruction for consumer records processes address both electronic media and hard copy records and include:
1. Period of retention for consumer records
2. Method used to determine record age
3. Processes used for actual record destruction
4. Documentation of record destruction activity, and
5. Individual responsible for initiating, managing, confirming, and documenting record destruction

The company maintains certifications that backed up data is encrypted and securely stored. The company back up process is to backup and store data which includes:
1. Limiting access to backup data to select authorized individuals
2. Secure transport of backup data to storage location, and
3. Security at the storage location

At a minimum this includes locked storage facility (when a physical building is used), secure access protocols, and compliance with all applicable legal and regulatory requirements.

The company destroys (render inaccessible/unreadable or unrecoverable) all consumer and customer information per all legal and regulatory requirements. The company utilizes on or more of the following destruction methods:
1. Burning, pulverizing, Shredding
2. Destroying or erasing electronic files, and/or
3. Utilizing a document destruction company that has been vetted by the company

<u>Incident Response</u>

The company maintains procedures for preventing, detecting, identifying, and responding to information system intrusions or any unauthorized access to computer systems or consumer data. The company utilizes various tools to prevent, and identify possible intrusions including one or more of the following:
1. Third party auditing results, intrusion detection testing results
2. Firewall protections
3. Website security, or
4. Other industry recognized security protocols and devices

The company maintains procedures to respond to information system intrusions including how consumer notification requirements are to be determined which Include the following:
1. Individual to contact in case of intrusion, plus back up personnel if needed
2. The need to stop any intrusion if still occurring
3. Determination of notification requirements
4. Preparing Notification
5. Securing approval of notification language (with legal if necessary)
6. Communicating the notification, and
7. Debrief to prevent future occurrences

Physical Security

The company maintains procedures which cover its employees, vendors and guests which controls access to areas that contain consumer information. The company procedures include:

1. Processes for granting levels of access to employees through keys, key fobs and/or security system passcodes
2. Procedures for authorizing and monitoring guests
3. Control of access for employees, vendors, and guests

Confidentiality

Access to confidential/sensitive consumer information is limited to those who have a legitimate need to know the information, which may be employees, vendors, and customers.

Vendors, Customers and Employees are vetted, educated, and provided with access necessary to their legitimate needs. All entities are under contract to keep information confidential. Consumers are vetted before information is disclosed to them. Employees are prohibited from browsing files or databases without a business justification. The company system retains logging information from each request for information and identifies each user requesting such information.

SafestHires, Inc.

Policy: Data Security Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is critical to protect consumer information from internal and external unauthorized access. There must be procedures maintained that include specifications for the securing of information when electronically transmitting information as well as information in hard copy and electronic form including information stored on portable and/or removable electronic devices. These procedures must meet all applicable legal and regulatory requirements.

Purpose

To avoid unnecessary risk and to ensure the safeguarding of consumer data, it is important to have very specific procedures outlined on controlling internal and external unauthorized access of information. The specific details should cover securing of information contained in hard copy and in electronic format including information stored on portable and/or removable electronic devices and should meet all applicable legal and regulatory requirements.

Scope

The scope of this policy includes all employees.

Policy

The company must protect consumer Information from internal and external unauthorized access. This Data Security Policy covers a wide scope of topics to protect against unauthorized access and to safeguard sensitive consumer information, which include but are not limited to:

Securing Unattended Workstations

The company requires employees to log out of computer systems as they leave their workstation. Paper files containing consumer information must also be secured when exiting the employee work area. The company employs screen savers that lock workstations after 15 minutes of inactivity.

Limited Access to Networks, Data and Work Areas

The company strictly requires t hat access to sensitive confidential consumer information be limited to those who have a legitimate need to know the information. Those with a legitimate need to have access to consumer information are vendors, certain employees, customers, and consumers who are the subject of the information. Such vendors, customers and employees are properly vetted and only provided access to consumer information to their specific legitimate needs and are contractually bound

to keep all information confidential. Consumers who are the subject of consumer reports prepared by the company and who contact us for information are also required to authenticate themselves prior to being provided with any information.

Secure Work areas Personnel

The company requires employees to use the company issued key/codes for access to perform employee required duties. Management reviews the level of physical access needed by employee and access levels may change based on job assignment. Employees are provided the lowest level of physical security access necessary to perform their job functions.

Visitors

All visitors moving beyond the front reception area are required to sign the visitor log registration upon arrival and must be checked out noting time when departing the office facility. The registration requires visitor name, date, time, purpose of the visit and party with whom they will be meeting with. While in the company office, visitors shall be escorted in areas where consumer information maybe visible on a computer screen or hard copy information is likely to be located.

Temporary Contract Workers

Temporary or contract workers are not granted access to areas that could contain consumer information that is not locked in a secure location. Any temporary or contract worker that is to be considered for a position the requires access to sensitive consumer information or to a secure area shall first undergo the same vetting/due diligence and execute the same confidentiality certification as are required for employees.

Limiting consumer information provided to information sources to only that which is needed for a specific business purpose

When the use of a consumer social security number and other sensitive information as required by law are needed internally or externally, the data exposed is limited to only that which is needed for the specific business purpose which has been identified.

Destruction of hard copy documentation

The company requires that all consumer related and customer related information per applicable legal and regulatory requirements be destroyed, be rendered inaccessible or unreadable and/or unrecoverable.

Identification of caller before providing consumer information

The company requires that all consumers be identified and authenticated prior to the disclosure of consumer information. Written records of information used to identify and authenticate consumers are

maintained.
The company procedure to authenticate consumers include, but is not limited to,
confirmation of full name as provided on consumer report and at least two of the following:

1. Date of Birth
2. Street address used on application or authorization document
3. Last four digits of SSN
4. Driver's License Number
5. Report ID Number

Employee Badging

Based on the current size of the company, employees recognize each other so employee badging is not needed. The company does require that unidentified individuals unaccompanied by another employee be reported immediately.

Unescorted Visitor Policy

The company maintains a Visitor Policy that requires all visitors to register upon arrival and check in when departing the office facility. This policy is written to ensure nonemployees do have access consumer information either in paper or electronically. While registering, visitors must inform the company their name, date, and time of visitor, who they will visit and the purpose of the visit. While on premise, all visitors must be escorted at all times as not to be left alone in work areas containing sensitive consumer information.

Secure Document Destruction

The company follows procedures to destroy, render inaccessible and unrecoverable all consumer and customer information as prescribed by the Federal Trade Commission Safeguards Rule.

Secure Transport of Information

The physical transport of consumer information is done for data backup purposes. The company policy is to secure information while in transit.

Use of Encryption and/or Secure Networks and/or Websites

The company policy is to protect all consumer information while in transit using no less than 256-bit SSL encryption. No consumer information is delivered over the internet that is not encrypted or secured with a minimum of 256-bit encryption. Users are required to maintain a confidential username and strong password.

Control of Access to Consumer Information

The company maintains a policy to help control access using strong passwords. Every employee is issued unique usernames for each system the employee is authorized to access. Employees are

required to set and maintain strong passwords which include a minimum of 8 characters, including capital letters, numbers, and special characters. Passwords must be changed every 6 months. Under this policy employees agree to treat passwords as confidential information and are prohibited from sharing this information with any party inside or outside of the company. Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

Controlling use of Portable Storage Devices

The storage of any consumer information outside the premises on any portable electronic storage device or media is strictly prohibited and contractually agreed to by employees with the one exception of secure transport of backup materials to an approved, vetted storage facility if needed. The company does not store data on portable devices.

Alarm Systems

The company office facility is secured by a monitored alarm system. The system is set for use whenever the office is closed for operations. Only authorized personnel have the alarm codes to disable the system. Employees are provided with adequate entry to areas in which they are authorized to perform their job. Employees do not have access to alarm system codes.

Door Locks

Entry doors to all secure areas are always locked during and after business hours. Only authorized personnel have entry rights to these areas. Employees maintain entry rights to areas in which they have been authorized to enter to perform job functions.

Secure Server and Back-Up Server

All backed up data is encrypted and stored in a secure facility separate from day-to-day operations. The company maintains certification of this storage and encryption.

SafestHires, Inc.

Policy: Intrusion and Data Security Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to follow procedures to prevent, detect, investigate, and respond to an information system intrusion, including consumer notification and other breach related notifications where mandated. These procedures must meet all applicable legal and regulatory requirements.

Purpose

To avoid unnecessary risk, it is essential that procedures be followed to prevent, detect, investigate, and respond to an information system intrusion. Such procedures must include consumer notification and other breach related notifications where necessary and must meet all legal and regulatory requirements.

Scope

The scope of this policy includes all employees.

Policy

The company maintains an Incident Response Policy which includes specific procedures to prevent, detect, investigate, and respond to an information system intrusion.

We have procedures for preventing, detecting, identifying, and responding to information system intrusions (unauthorized access to computer systems and/or consumer data). Our tools used to prevent, detect, and identify intrusions include one or more of the following:

- Third-party audit results, intrusion/detection testing results,
- Firewall protections,
- website security, or
- other recognized security protocols and devices.

We also have a procedure/system in place to respond to any information system intrusions, including how consumer notification requirements are determined. Specifically, we include some or all, but not limited to, the following:

- Individual to contact in case of intrusion and his/her back-ups,
- Necessity of immediately stopping intrusion activity, if still occurring,
- Determination of notification requirements,
- Preparing notification,
- Obtaining necessary approvals of notification language,

- Communicating notification, and
- Debrief to prevent future occurrences

The company policy and procedures on information system intrusion meet all applicable legal and regulatory requirements.

SafestHires, Inc.

Policy: Storage and Backup of Data Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as “the company”.

Overview

It is important to follow procedures to ensure data is backed up and stored in an encrypted or otherwise protected manner. These procedures must meet all applicable legal and regulatory requirements.

Purpose

To avoid unnecessary risk, it is important to ensure data is backed up and stored in an encrypted or otherwise protected manner.

Scope

The scope of this policy includes all employees.

Policy

The company maintains policy and procedures to ensure data is backed up and stored in an encrypted or otherwise protected manner.

The company maintains certification that our backup data is encrypted and securely stored.

Our process to back up and store data includes:
1. Limiting access to backup data to select authorized individuals.
2. The Secure transport of backup data to storage location (including virtual storage) and security at the storage location.
3. At a minimum this includes locked storage facility (if physical building is used) secure access protocols and compliance with all applicable legal and regulatory requirements.

SafestHires, Inc.

Policy: Access Protocol Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

It is important that procedures be followed regarding the use of secure access protocols for employees, authorized customer users and any other authorized users with access to consumer information. Such procedures must meet all applicable legal and regulatory requirements.

Purpose

To avoid unnecessary risk, procedures must be followed to ensure there are secure access protocols in place for authorized users with access to consumer information including employee and customer users.

Scope

The scope of this policy includes all employee.

Policy

The company maintains access protocols to control access to consumer information to authorized users only which include authorized employees and authorized customers. Such protocols include but are not limited to the following:

1. Strong Password with automatic notification of password change requirements)
2. Biometric identification, and/or
3. Multifactor authentication

The company maintains documentation on authorized parties with access and access is reviewed regularly.

SafestHires, Inc.

Policy: Electronic Access Control Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

It is important to maintain procedures to control access to all electronic information systems and electronic media that contain sensitive consumer information. Such procedures should include processes to administer access rights based on roles and job functions. Employees and authorized end user customers must only be given the access levels necessary to perform their required functions. Access rights must be monitored regularly and updated based on personnel or system changes.

Purpose

To avoid unnecessary risk and to avoid any form of breach in data security, it is important to control electronic systems access to ensure access rights are only provided at levels necessary for employees and authorized end users to perform their required functions.

Scope

The scope of this policy includes all employees.

Policy

The company maintains processes to control and administer access rights to electronic systems and media that contain sensitive consumer information. The company only grants system access for employees and authorized end users which is necessary to perform required job functions.

The company Chief Technology Officer is responsible for controlling access to consumer information and he is able to document the process for granting access and for adding and changing levels of access based on job functions and the need for information.

Procedures for granting system access include:
1. Employees officially request for access to certain electronic systems and/or media. Request is reviewed and either approved or denied. No access may be granted until it is reviewed and approved.
2. Written authorization is provided to document the approval for access.
3. User logins and passwords are generated and issued to users as applicable
4. Access rights are monitored and reviewed regularly by the company, and when employees have a change in position.
5. Access is terminated immediately upon discovery the employee no longer has a legitimate business need for a system or electronic media access.

SafestHires, Inc.

Policy: Physical Security Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as “the company”.

Overview

It is important to maintain procedures to control physical access to all office areas including data storage facilities that contain sensitive consumer information.

Purpose

To avoid unnecessary risk and to avoid any form of breach in data security, it is important to control physical access to all appropriate office areas containing sensitive consumer information

Scope

The scope of this policy includes all employees.

Policy

The company maintains policy and procedure on physical access control that controls access to areas that contain sensitive consumer information. The company procedures include but are not limited to the following:

1. Processes for granting levels of access based on job duties and assignment of appropriate access methods including keys, and passcodes
2. Processes for authorizing and monitoring visitors
3. Control of access by employees, vendors, and visitors

All visitor registry records are maintained for a minimum of one year.

SafestHires, Inc.

Policy: Consumer Information Privacy Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	Confidential

SafestHires, Inc is hereinafter referred to as "the company".

Overview

It is important to follow a Consumer Information Privacy Policy detailing the purpose of the collection of consumer information, the intended use and how the information will be shared, stored, and destroyed. This policy must be visible on a company website for access by customers and/or consumers and made available for distribution upon request.

Purpose

To avoid unnecessary risk, it is important to detail the purpose of the collection of consumer information, its intended use and how the information will be share, stored, and destroyed. It is important this information should be made public on a website and made available upon request.

Scope

The scope of this policy includes all employees.

Policy

The company maintains a Privacy Policy which is reviewed and updated at least annually and more frequently as necessary. The company Privacy Policy is located on its website at: www.safesthires.com/privacy-policy/

The company Privacy Policy is made available to any party requesting a copy utilizing methods other than the company website.

The policy includes information on the following topics:
1. The purpose of the collection of consumer information
2. The intended use of consumer information
3. How the information is shared, stored, and destroyed

SafestHires, Inc.

Policy: Unauthorized Browsing Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

It is essential to follow a policy that prohibits employees from searching files and databases unless there is a legitimate business need to do so.

Purpose

To avoid unnecessary risk, and to ensure the safeguarding of consumer information it is important that employees not be allowed to browse files or databases unless there is a legitimate business purpose which is authorized.

Scope

The scope of this policy includes all employees.

Policy

The company maintains Policies and Procedures which instructs employees on acceptable use. Employees are strictly prohibited from browsing or searching files and databases unless they have a legitimate business purpose. The company employee handbook covers acceptable use and states unauthorized browsing of files and databases is prohibited.

SafestHires, Inc

Policy: Record Destruction Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is essential to have procedures to destroy or properly dispose of records containing sensitive consumer information. Such procedures must meet all applicable legal and regulatory requirements including but not limited to the Federal Trade Commission's Safeguards Rule. Records containing sensitive consumer information must be destroyed and unrecoverable.

Purpose

To avoid unnecessary risk, and to safeguard sensitive consumer information, all records containing sensitive consumer information must be destroyed so they are unrecoverable.

Scope

The scope of this policy includes all employees.

Policy

The company maintains processes to destroy, render inaccessible/unreadable and/or unrecoverable all consumer and customer information. The following methods are utilized:

1. Burning, pulverizing and/or shredding
2. Destroying or erasing electronic files

Document destruction companies are properly vetted prior to performing services for the company. As part of the vetting process, the company performs interviews with the company, perform a telephone verification look up through online sources or the yellow pages, confirm company website and business license. In the interview the company requires references from document destruction firms. The company requires a confidentiality certification to be included in a service level or separate standalone agreement.

The company requires employees to remove all hard paper copies of consumer information be removed from work areas when leaving the space and that all consumer information printed in hard copy be destroyed immediately once the information is no longer needed for legitimate business purposes,

SafestHires, Inc.

Policy: Sensitive Data Masking Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to have procedures to suppress or truncate social security numbers and other sensitive data elements as required by law. If an end user of the consumer data requires full social security numbers or other sensitive data elements, a certification from that end user must be obtained which confirms the end user will comply with all applicable legal and regulatory requirements regarding its use, safeguarding and destruction of such information.

Purpose

To avoid unnecessary risk, it is essential to maintain procedures that suppress, or truncate social security numbers and other sensitive data elements as required by law. Should end users require the display of this data, certifications must be obtained to confirm compliance with all applicable legal and regulatory requirements regarding its use, safeguarding and destruction.

Scope

This policy includes all employees.

Policy

The company maintains procedures that forbid the communication of more than the final four digits of consumer social security numbers in any form outside of the company environment unless an approved exception exits.

If the exception is due to an end user requirement, the company requires the end user to certify in writing they will comply with all applicable legal and regulatory requirements regarding its use, safeguarding and destruction.

When the use of a social security number or other sensitive data elements is required internally or externally, the data exposed is limited to only that which is needed for a specific business purpose identified and approved by the company.

When communicating social security numbers or other sensitive data elements as required by law or required business purpose approved by the company, secure transport methods are used to deliver the information

End user written certifications are retained in customer files during the relationship with the customer and no less than 7 years after termination.

SafestHires, Inc.

Policy: Legal and Regulatory Requirements Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTAIL

SafestHires, Inc. is hereinafter referred to as "the company".

Overview

The company must comply with all provisions of all applicable law and regulation in providing its consumer reports for screening purposes. This includes but is not limited to the federal Fair Credit Reporting Act (FCRA), the federal Gramm-Leach-Bliley Act (GLBA) and all legal and regulatory requirements identified in the Professional Background Screeners Association Accreditation Standard.

Purpose

It is critical that the company demonstrate that its employees have a thorough understanding of all legal requirements in providing its products and services to the marketplace. The purpose of this policy is to detail the training and assessment processes required to demonstrate competency with legal and regulatory requirements.

Scope

The scope of this policy includes all employees and is ongoing throughout employment with the company.

Policy

As a condition of employment with the company, all employees are required to participate in certain required trainings and demonstrate evidence of knowledge on industry legal and regulatory requirements. Trainings are required for new hires and continue during the duration of employment. Trainings will include but not be limited to regulations such as the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act and all regulatory requirements identified in the Professional Background Screeners Accreditation Standard.

Employees can demonstrate knowledge of the company compliance requirement and are able to access a current copy of documentation. Employees know and understand the designated individual responsible for legal and regulatory compliance for the company is Andrew Andersen. Employees are required to maintain a Fair Credit Reporting Act Certification through the Professional Background Screeners Association. New hires are expected to earn this certification within the first 3 months of employment. All new hires are provided with a data security awareness training before they are provided with access to consumer confidential information.

Continuing compliance education is made available through the following resources: attendance at Professional Background Screeners Association webinars and conference events, industry publications, vendor notifications.

SafestHires, LLC

Policy: Federal Consumer Reporting Law Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as "the company".

Overview

It is important to designate one responsible party for oversight, development, implementation and ongoing compliance with the federal Fair Credit Reporting Act and any other federal applicable laws that pertain to consumer reports delivered by the company for employment purposes.

Purpose

Having one individual responsible for the overall compliance with state and federal consumer reporting laws creates authority and responsibility for training, the potential for future changes in process and efficiency in communications.

Scope

The scope of this policy includes the responsible party as well as all employees within the company. All employees need to be aware of who holds this responsibility that party is available as a resource.

Policy

The company maintains a written job description identifying Andrew Andersen as the party responsible for the development, implementation, and on-going compliance with the federal Fair Credit Reporting Act and any other federal applicable laws that pertain to consumer reports delivered by the company for employment purposes.

As the responsible party, Andrew Andersen has offered a signed affidavit affirming his responsibility and that he is qualified to hold this position within the company. As further evidence of his qualification, he has provided his credentials which include his Advanced FCRA Certification with the Professional Background Screeners Association.

SafestHires, LLC

Policy: State Consumer Reporting Law Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as "the company".

Overview

It is important to designate one responsible party for oversight, development, implementation, and ongoing compliance with all state consumer reporting laws that pertain to consumer reports provided by the company for employment purposes.

Purpose

Having one individual responsible for the overall compliance with state consumer reporting laws creates authority and responsibility for training, the potential for future changes in process and efficiency in communications.

Scope

The scope of this policy includes the responsible party as well as all employees within the company. All employees need to be aware of who holds this responsibility that party is available as a resource.

Policy

The company maintains a written job description identifying Andrew Andersen as the party responsible for the development, implementation, and on-going compliance with the state laws that pertain to the consumer reports provided by the company for employment purposes.

As the responsible party, Andrew Andersen has offered a signed affidavit affirming his responsibility and that he is qualified to hold this position within the company. As further evidence of his qualification, he has provided his credentials which include his Advanced FCRA Certification with the Professional Background Screeners Association.

SafestHires, Inc.

Policy: Driver Privacy Protection Act (DPPA) Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as “the company”.

Overview

It is important to designate one responsible party for oversight, development, implementation, and ongoing compliance with the Drivers Privacy Protection Act (DPPA) that pertain to the consumer reports provided by the company for employment purposes.

Purpose

Having one individual responsible for DPPA regulation creates authority and responsibility for training, the potential for future changes in process and efficiency in communications.

Scope

The scope of this policy includes the responsible party as well as all employees within the company. All employees need to be aware of who holds this responsibility, and that party is available as a resource.

Policy

The company maintains a written job description identifying Andrew Andersen as the party responsible for the development, implementation, and on-going compliance with all DPPA regulation that pertain to the consumer reports provided by the company for employment purposes.

As the responsible party, Andrew Andersen has offered a signed affidavit affirming his responsibility and that he is qualified to hold this position within the company.

SafestHires, Inc.

Policy: State DPPA Compliance Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as “the company”.

Overview

It is important to designate one responsible party for oversight, development, implementation, and ongoing compliance with state statues for the Drivers Privacy Protection Act (DPPA) that pertain to the consumer reports provided by the company for employment purposes.

Purpose

Having one individual responsible for state DPPA regulation creates authority and responsibility for training, the potential for future changes in process and efficiency in communications.

Scope

The scope of this policy includes the responsible party as well as all employees within the company. All employees need to be aware of who holds this responsibility, and that party is available as a resource.

Policy

The company maintains a written job description identifying Andrew Andersen as the party responsible for the development, implementation, and on-going compliance with all state DPPA regulation that pertain to the consumer reports provided by the company for employment purposes.

As the responsible party, Andrew Andersen has offered a signed affidavit affirming his responsibility and that he is qualified to hold this position within the company.

SafestHires, Inc.

Policy: Integrity Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as the "the company".

Overview

It is critical the company have a companywide policy against committing the act of bribery or any other fraudulent activity to obtain preferential treatment from a public official or a government entity. These behaviors cannot not be tolerated. All employees need to be informed to make good common-sense judgment as it pertains to avoiding situations involving bribery and maintaining the highest integrity standards.

Purpose

Since inappropriate, low integrity behaviors should not be tolerated, it is important to specify exactly what is not allowable during employment with the company. The purpose of this policy is to detail unacceptable behavior to maintain the overall integrity of the company.

Scope

The scope of this policy includes all staff as it pertains to interactions with public officials or government entities.

Policy

Bribery or any fraudulent activity to obtain preferential treatment from a public official is expressly prohibited. Any employee known to violate this prohibition will be subject to disciplinary action up to and including immediate termination of employment with the company.

This Anti bribery requirement is communicated to employees through various company training events. It has been verified that the company, its principals, or employees have not been convicted of bribery or other fraudulent activity.

SafestHires, Inc.

Policy: Prescribed Notices Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as "the company".

Overview

Operating as a consumer reporting agency it is essential the company provide customers current versions of all currently required federal notices required by the federal Fair Credit Reporting Act, such as those prescribed by the CFPB.

Purpose

To avoid unnecessary risk it is essential the company provide customers with all required federal notices and requirements under the Fair Credit Reporting Act including Notices to Users, Obligations of Users and A Summary of Your Rights under the Fair Credit Reporting Act. Acknowledging receipt of such notices serves as evidence that customers have been informed.

Scope

The scope of this policy includes all customers and all employees responsible for writing, disseminating, collecting, and storing of customer agreements and training material.

Policy

The company provides all required FCRA notices including the Notice to End Users of Consumer Reports, Obligations of Users under the FCRA and A Summary of Your Rights Under the Fair Credit Reporting Act to every customer. Customers are not allowed access to consumer reports prior to receiving these notices and prior to acknowledging receipt.

These required notices are provided to customers as part of the new customer package which are made available through the Company technology and includes a version which can be downloaded by users. Customers are required to acknowledge receipt of all notices in their service agreements. Customers are also provided the notices again during the training provided as a new customer.

SafestHires, Inc.

Policy: Customer Agreement Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as "the company".

Overview

Operating as a consumer reporting agency it is essential to obtain a signed agreement, certification, affirmation, or other signed document from customers (users according to the federal Fair Credit Reporting Act) in which the customer agrees to meet the requirements of all applicable law and regulation, specifically but not limited to the federal Fair Credit Reporting Act.

Purpose

To avoid unnecessary risk it is important to have signed agreements that spell out all customer obligations and legal requirements under the FCRA, and that contain certifications the customer will comply.

Scope

The scope of this policy includes all customers and all employees responsible for writing, disseminating, collecting, and storing of customer agreements.

Policy

The company requires customers to execute a service agreement before access to consumer reports is granted. The company service agreement contains stipulations to comply with applicable state and federal laws and specifically states the following requirements:

1. The customer must have a permissible purpose for ordering and receiving consumer reports
2. Customer agrees to comply with disclosure and authorization requirements
3. Customer agrees to comply with adverse action required procedures
4. Customer understands the confidential nature of the information being requested and will keep it confidential when obtaining, retaining, using, and destroying
5. Customer will comply with all laws and regulations
6. Customer will not use consumer reports in violation of any state or federal law

The company agreement is available through the technology online application system which includes links to the service agreement. The company requires its service agreement be executed by an authorized representative of the customer's organization. All agreements received from customers are reviewed to ensure no modifications or alterations have been made. Access to consumer information may not be granted unless customer agrees to all its requirements under the federal Fair Credit Reporting Act. Agreements are retained for the duration of the customer relationship and not less than 7 years after the termination of access to consumer reports.

SafestHires, Inc.

Policy: Customer Legal Responsibility Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as the "the company".

Overview

It is critical the company inform all customers they have legal responsibilities when procuring and using consumer reports for employment purposes. A consumer reporting agency must recommend that customers work with legal counsel to ensure compliance with their specific legal responsibilities.

Purpose

To avoid unnecessary risk, it is critical to inform customers they have legal responsibilities within the federal Fair Credit Reporting Act when procuring and using consumer reports for employment purposes and that they should consult with legal counsel to ensure compliance with their specific responsibilities.

Scope

The scope of this policy includes all employees who draft customer agreements and who draft and disseminate training materials.

Policy

The company informs customers they have legal responsibilities when using consumer reports for employment purposes. Specifically, the company informs customers of the following through customer agreements and written training materials:

1. Consult with legal counsel and remain compliant with their own legal responsibilities
2. Always have a permissible purpose before requesting a consumer report
3. Make a disclosure to the consumer
4. Obtain consumer authorization
5. Follow prescribed adverse action procedures
6. Comply with all applicable legal and regulatory requirements
7. Obtain, retain use, and destroy consumer information in a compliant and confidential manner

The company requires customer agreements to be executed by an authorized representative of the customer prior to receiving access to consumer reports. All customer agreements are checked to ensure no alterations or modifications have been made to the customer legal responsibility statements as no omissions or alterations to customer responsibilities are acceptable. All customer agreements are retained in hard and electronic format and kept for the duration of the relationship with the customer. Agreements are then retained for not less than 7 years after the termination of the customer relationship and access to consumer reports.

SafestHires, Inc.

Policy: Customer Required Documents Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as the "the company".

Overview

It is critical the company inform customers of specific forms or documents required to complete specific consumer report related searches

Purpose

To avoid unnecessary risk and to minimize delays in turn around times in it essential the company inform customers of specific forms or documents necessary to complete specific searches.

Scope

The scope of this policy includes all employees that prepare customer training material and who conduct customer trainings.

Policy

The company provides customers with specific forms or documents required to complete specific searches to which they will have access during the onboarding/training session with new customers. Electronic versions of these forms are also available for customers. If a particular vendor or jurisdiction or other source implements new required forms, customers are notified and supplied with the new required forms or documents.

The following is an example of form requirements that are communicated to customers:
1. Any required forms and/or information to obtain statewide criminal record searches in states that currently require specific forms and/or information
2. Any required forms and/or information to obtain driving records in those states that currently require specific forms and/or information
3. Any other specific disclosure and authorizations needed to obtain a specific report

SafestHires, Inc.

Policy: Disclosure and Authorization Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to inform customers of legal requirements imposed by the federal FCRA and, in some instances, state consumer reporting laws regarding disclosing to and obtaining authorization from consumers prior to requesting a consumer report from the company. Recommendations must be made to customers to consult with legal counsel to develop a legally compliant disclosure and authorization process.

Purpose

To avoid unnecessary risk and delays in turn around time it is critical that the company inform customers of their legal requirements on consumer disclosures and authorizations. Specifically, customers should be informed they need to disclose to and receive authorizations from consumers before requesting consumer reports and that they should always consult with legal counsel on these matters and to develop a legally compliant disclosure and authorization internal process.

Scope

This policy includes employees who draft customer agreements and who draft and facilitate customer training material.

Policy

The company informs customers of their disclosure and authorization legal requirements imposed by the federal FCRA and some state reporting laws by way of its customer agreement, executed by the customer. We provide a sample Disclosure and Authorization form containing specific requirements during the initial onboarding training and update these samples when advisable for their use in discussion with customer legal counsel.

The customer agreement advises clients to consult with legal counsel to ensure that customer's practices and procedures related to the use of company provided information (including Disclosure and Authorization requirements) are in full compliance with all applicable state and federal laws.

SafestHires, Inc.

Policy: Adverse Action Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to inform customers of their legal requirements imposed by the federal Fair Credit Reporting Act, and in some instances, state consumer reporting laws regarding taking adverse action against a consumer based on a consumer report. It is also important to recommend customers consult with legal counsel to develop a legally compliant adverse action process.

Purpose

To avoid unnecessary risk, it is important that customers be informed of their legal requirements imposed by the federal FCRA and in some cases, state consumer reporting laws which require adverse action obligations when taking an adverse action on a consumer based on a consumer report. Equally as important is the need to recommend that customers seek legal consultation to develop a legally compliant adverse action process.

Scope

The scope of this policy includes employees who draft customer agreements and draft and facilitate customer trainings.

Policy

The company informs all customers there are legal requirements and responsibilities when taking adverse action based in whole or in part on consumer reports. Customers are informed and agree to comply with adverse action procedures as required by the FCRA including the requirement to provide a preliminary adverse action notice to consumers, along with a copy of the consumer report and A Summary of Your Rights under The Fair Credit Reporting Act, allowing the consumer a designated period of time to contact the company if the consumer wishes to dispute any information contained within the consumer report, providing the company contact information and providing a final adverse action notice to the consumer if/when a final adverse employment decision is made. This information is communicated to customers through the company customer agreement.

Also included in the company customer agreement is the recommendation to consult with legal counsel regarding specific legal responsibilities and for the development of a compliant adverse action process. We require customer agreements to be executed by authorized representatives and prior to providing access to consumer reports. Executed customer agreements are reviewed to ensure no alterations or modifications were made to the adverse action or consultation with legal counsel language as no modifications are acceptable and access to consumer reports may not be granted with any changes to company agreements.

SafestHires, Inc.

Policy: Truth in Advertising Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

It is important to inform customers about information source types, limitations, variables affecting information available and scope of information within each consumer reporting product.

Purpose

To avoid unnecessary risk, it is critical to communicate to customers information about how information is collected from what sources and methodologies utilized. This helps to set accurate expectations in the information being delivered to the customer.

Scope

The scope of this policy includes all employees.

Policy

The company provides information containing the nature of the original source, limitations, variables affecting the information available, and scope of information provided by each consumer reporting product offered. Specifically:

- The identification of the information source
- Type of source
- Scope of records searched
- Search methodology

Our procedure is to include these notices with the new customer start up materials and clients are not granted access to reports until after they have received these notices/materials.

We utilize a detailed product proposal that we send to all prospects which includes a brief description of our products. This information also contains identification of information sources, types of sources, the scope of records searched and search methodologies.

SafestHires, Inc.

Policy: Legal Counsel Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as "the company".

Overview

It is essential to inform customers the importance of working with legal counsel to develop an internal employment screening program specific to their needs and to ensure their policies and procedures related to the use of consumer reports is compliant with all applicable legal and regulatory requirements. The communication must include a statement that the consumer reporting agency does not act as legal counsel and cannot provide legal advice.

Purpose

To avoid unnecessary risk, it is critical to communicate to customers the recommendation to seek legal counsel and to develop an employment screening program specific to their needs and that is compliant with local, state, and federal regulations. This communication should include a statement that the consumer reporting agency does not act as legal counsel and cannot provide legal advice.

Scope

The scope of this policy includes all employees that process consumer reports and who are responsible for creating customer service agreements and training materials.

Policy

The company ensures that customers are informed the company does not act as legal counsel or provide legal advice. The company also informs customers they should seek their own legal counsel to develop an employment screening program specific to their needs and to ensure their policies and procedures related to the use of consumer reporting is compliant with all local, state, and federal legal and regulatory requirements. Information provided to customers also advises them that consumer reports provided by the company must be used in compliance with all applicable legal and regulatory requirements.

This information is provided to customers in the company end user agreement for service and in new customer onboarding training material. The company requires the end user agreement is executed by an authorized representative before access to consumer reports can be provided. The company does not accept any alterations or modifications to the end user agreement for service that in anyway alters or changes these statements.

SafestHires, Inc.

Policy: Understanding Consumer Reports Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTAIL

SafestHires, Inc is hereinafter referred to as “the company”.

Overview

It is important to provide guidance to customers on how to order, retrieve, read and understand the information provided in consumer reports.

Purpose

To avoid unnecessary risk, it is important that all customers be properly educated on the ordering, the retrieving, the reading and understanding of consumer reports.

Scope

The scope of this policy includes all employees who prepare consumer reporting, who provide customer service to customers and who are responsible for preparing training materials for customers.

Policy

The company provides necessary customer training assistance through the new customer onboarding training process and through the relationship with the customer as may be necessary as new staff is hired or responsible for ordering, receiving, reading and understanding consumer reports.

The following methods are used to provide customers with instructions and guidance:

1. User manual
2. Videos
3. Verbal Assistance – Support contacts within the company to contact for future assistance
4. User training classes or webinar(s)

All written instructions are reviewed not less than annually for currency and are updated as necessary as changes in order or delivery methods change.

SafestHires, Inc.

Policy: Information Protection Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as “the company”.

Overview

It is important to provide customers with information on the sensitive nature of consumer reports, the requirement to protect this information and the consumer report retention and destruction requirements under the FCRA and the DPPA.

Purpose

To avoid unnecessary risk, it is important to inform customers of the sensitive nature contained with consumer reports, their requirement to protect and secure this information and the retention and destruction requirements that must be followed.

Scope

The scope of this policy includes all employees who prepare consumer reports, all staff responsible for writing customer service agreements and all staff responsible for writing customer training material.

Policy

The company provides its customers with sufficient information regarding their obligations for retention and destruction of consumer information under the FCRA and DPPA. All customers understand the sensitive nature of consumer reports, the need to protect the information and the consumer report retention and destruction practices outlined by the FCRA and DPPA. We offer a guide to using background reports through a link in our welcome email to new customers and in our company customer service agreements provided to our customers, they agree to:

Limit dissemination of consumer information to only those with legitimate need, permissible purpose, and authorized by consumer

Retain consumer data in a confidential manner

Destroy data in a secure manner to make it inaccessible, unreadable, and/or unrecoverable by:

- burning, pulverizing, or shredding,
- destroying or erasing electronic files, and/or
- after conducting due diligence, hire a document destruction company. In addition, paper documents containing personally identifiable information (particularly name, date of birth, and SSN), if retained at individual desks/workstations, shall be destroyed or inaccessible no later than the end of each workday

Protect the privacy of consumer information which is contained in motor vehicle records, and access DMV records only with written consent of consumer.

The company requires our Customer Agreement be signed by an authorized representative of the client prior to client being given access to request or receive any consumer reports from us. The Customer Agreement is checked to ensure no modifications have been made by the client. If modifications have been made, the customer will not be granted ordering or receiving privileges. Under no circumstances will any changes to consumer information protections be accepted.

SafestHires, Inc.

Policy: Public Record Researcher Agreement Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: 5/18/2021
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

It is important to have signed agreements from all non-employee public record researchers. Such agreements must define the scope of services to be provided, including jurisdictions covered, searching methodology, depth of search, disclosure of findings, methodology and time frame for communication and completion of requests, methodology for confirming the identity of the subject of record(s), confidentiality requirements, reinvestigation requirements, and other obligations as furnishers of information under the federal Fair Credit Reporting Act.

Purpose

To avoid necessary risk, all non-employees who are tasked as public record researchers should confirm roles and responsibilities through an agreement. This will eliminate any questions of responsibility or expectation of the researcher and his/her performance.

Scope

The scope of this policy includes all employees that prepare consumer reports, and employees who perform quality analysis auditing on third party public record researchers.

Policy

The company provides every non-employee, third party public record researcher with a standard agreement as confirmation of the service level expectations required to perform their work. Such agreements must be executed by an authorized representative and no alterations or modifications are accepted to the service level requirements. Under no circumstances
are any non-compliant changes or corrections allowed to the following topics included in the agreements:

1. The requirement to conduct all searches in full compliance with applicable law and regulation,
2. Jurisdictions covered,
3. Search methodology,
4. Depth of search,
5. Disclosure of findings
6. Methodology and time frame for communication and completion of requests,
7. Methodology for confirming identity of subject of record(s),
8. Confidentiality requirements,
9. Reinvestigation requirements,
10. Other obligations as a furnisher of information under the federal FCRA, and

11. The requirement for public record researcher to obtain a similar agreement from subcontractors if subcontracts are used. If applicable this agreement must include:

A. the legal requirement to treat all consumer information as confidential,
B. secure data transmission, and
C. secure and timely disposal of confidential information

SafestHires, Inc.

Policy: Researcher Vetting Requirement Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as “the company”.

Overview

As a consumer reporting agency, it is important to vet or credential every public record researcher prior to using their services. All public record researchers must pass the requirements to be considered a service provider.

Purpose

To avoid unnecessary risk, it is essential that every public record researcher undergo certain credentialing or vetting prior to performing services for the company.

Scope

This policy includes all employees responsible for the credentialing of third party service providers including public record researchers.

Policy

The company performs a credentialing/vetting function on all new public record researchers prior to the researcher performing services on behalf of the company.

The company process to perform due diligence on the researcher includes (but not limited to) collecting the following:

1) evidence of right to conduct business, such as copy of business license, articles of incorporation, state filing etc., and authentication thereof,

2) verification of required private investigator license if such license is required and

3) results of test searches conducted.

The vetting records may include but are not limited to:

1) completed favorable reference interviews from at least one current client,

2) verification of association memberships such as local Chamber of Commerce, Better Business Bureau, NCISS, ASIS, and/or PBSA and

3) confirmation of certification received by successfully completing the "PBSA RESEARCH PROVIDER EXAMINATION.”

All public record researcher credentialling/vetting documentation is maintained in the vendor file.

SafestHires, Inc.

Policy: Public Record Researcher Certification Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to require that all public record researchers certify in writing they will conduct their research in compliance with all applicable legal and regulatory requirements, as well as in the manner prescribed by the repository which maintains the office record of the court. The certification should confirm the researcher will never obtain information through illegal or unethical means and will utilize document disposal and/or destruction methods prescribed in the federal Fair Credit Reporting Act.

Purpose

To avoid unnecessary risk, all public record researchers must certify in writing by executing an agreement they agree to comply with all applicable legal and regulatory requirements in the manner prescribed by the repository, they will obtain information through legal and ethical means, will dispose of information confidential in nature through secure means per the Federal Trade Commission destruction rule, will transmit all consumer information securely and allow for regular auditing.

Scope

The scope of this policy includes all employees responsible for adding or managing public researcher relationships and employees responsible for writing agreements for third party relationships.

Policy

The company requires all public record researchers tasked with performing court research execute a Public Record Researcher Agreement. Only authorized representatives of the researcher are allowed to sign the agreement and no alterations or modifications to the requirements outlined within the agreement are allowed. Executed agreements collected from Public Record Researchers are maintained in the company vendor files throughout the business relationship. Under no circumstances will any non-compliant changes be allowed to the following requirements called for in the researcher agreement:

1. Researcher agrees to comply with all legal and regulatory requirements, as well as in the manner prescribed by the repository which maintains the official record of the court,
2. Researcher agrees to obtain information only through legal and ethical means,
3. Researcher agrees to dispose of or destroy confidential documents in a secure manner per the Federal Trade Commission (FTC) document destruction rule,
4. Researcher agrees to transmit all consumer information in a secure manner, and
5. Agrees to the company right to audit as necessary and agrees to fully cooperate and participate as required.

SafestHires, Inc.

Policy: Researcher Errors and Omissions Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to obtain proof of public record researcher Errors and Omissions insurance coverage. It is also important to work only with those researchers who can provide proof of insurance, denying any researchers who cannot adequately supply this evidence.

Purpose

To avoid unnecessary risk, it is essential that all public record researchers performing searches supply ongoing evidence of adequate errors and omissions insurance coverage.

Scope

The scope of this policy includes all employees responsible for vetting and reviewing public record researchers.

Policy

The company requires due diligence and vetting of all public record researchers before the use of their services and again annually thereafter. We verify the researcher's Errors and Omissions insurance coverage and require a minimum of one million dollars in coverage and that the company be notified immediately should coverage be dropped, or the amount of coverage changed to below one million dollars. Evidence of insurance is required through the insurance declarations page supplied by the researcher. The declarations page is required to be supplied to the company annually while performing searches for the company. All researcher insurance information is maintained in the company vendor files.

SafestHires, Inc.

Policy: Researcher Information Security Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important provide a secure method and require such a secure method be used by public record researchers to receive orders and return search results. The use of a secure method for the delivery of sensitive consumer information (Personally Identifiable Information) is required.

Purpose

To avoid unnecessary risk, it is essential that public record researchers agree through an executed agreement to receive and deliver consumer information securely to ensure the safeguarding of consumer information.

Scope

The scope of this policy includes all employees responsible for writing third party public researcher agreements.

Policy

The company requires the secure transmission of any/all sensitive consumer information (Personally Identifiable Information) sent to or received from public record researchers. The company requires that all public record researchers execute a signed agreement in which they agree to the following:

1. Use of an electronic system designated for secure transmission of information between the company and the researcher. The company recommends the use of its technology for all such transmissions however, if a different transmission method is used for any reason, the following security protocols must include:
   A. All transmissions must be directed to a specific named party,
   B. All transmissions must be clearly marked as "Confidential" and include a request to notify the sender if received by another party,
   C. If faxed, a cover page must always be included and must not contain any sensitive consumer information (Personally Identifiable Information),
   D. If faxed, the company must have verified receiving fax is in a non-public location,
   E. If transmitted through the internet, data must be encrypted with a minimum of 256-byte encryption.

The company requires the agreement be executed by an authorized representative and that no alterations or modifications are made to these requirements. All executed public researcher agreements are maintained in the third-party vendor file throughout the duration of the relationship.

SafestHires, Inc.

Policy: Researcher Auditing Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires Inc is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to audit public record researchers regularly for quality control purposes. It is essential that all public researchers agree to ongoing auditing of work performed to confirm the quality of information being supplied.

Purpose

To avoid unnecessary risk, it is important to have processes that include the ongoing monitoring of all public record researchers to ensure the quality of information returned. The auditing practice must include the recommendations for corrective actions that may become necessary if lapses in quality are discovered.

Scope

The scope of this policy includes all employees that prepare consumer reports and all employees that process the auditing requests of public record researchers.

Policy

The company audits all public record researchers to ensure the quality of their work. As we perform public record researcher audits the company procedures include—but are not limited to:

1) an established protocol for auditing researchers,

2) volume of audit to be conducted,

3) sending research requests where result is already known,

4) how returned results are compared to expected results, and

5) process for dealing with researcher errors up to and including termination of services.

The company retains researcher audit results for a minimum of one year. Each researcher audit is logged and contains the following details:

1. Date of Test
2. Unique Identifier such as order number or subject name and last 4 digits of SSN
3. Results Returned
4. Report on findings, whether the report was as expected or not
5. Any remedial actions taken or notes on conversations with researcher

The frequency of researcher audits is based on volume of searches performed by researcher. In general audits are to be performed on .25% of researcher volume, not more than once every month for high volume researchers and not more than once every year for low volume researchers.

To begin the researcher audit, a duplicate request is place through an alternate source. Results are compared between researchers and discrepancies or differences between the results are logged and investigated. If the audited researcher erred, the nature of the error is reviewed to determine if it was a false positive or false negative. The results are discussed with the researcher for any corrective actions to be taken in the future to avoid either the false positive or negative. Researchers with any discrepancies noted are audited more often to ensure no additional discrepancies are noted. If the researcher continues to fail with continual patterns or mistakes, the company will terminate the services from that researcher.

SafestHires, Inc.

Policy: Verification Accuracy Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to assure maximum possible accuracy when obtaining, documenting, and reporting verification information for consumer reports. Certain procedures should be followed to ensure verification accuracy and employees responsible for verification accuracy need to be provided with adequate training.

Purpose

To avoid unnecessary risk, reasonable procedures need to be followed to assure maximum possible accuracy when obtaining, documenting, and reporting verification information for consumer reports.

Scope

The scope of this policy includes all employees that obtain, document and report verification information and employees responsible for employee training.

Policy

The company maintains procedures designed specifically to reasonable ensure verifications accuracy. When providing verifications of academic, employment, reference or other checks which are not public in nature, we always verify accuracy with processes to ensure the identity of the subject of the search, identify of the provider and the completeness/accuracy of the data itself.

The company confirms the subject identity through a verification of the social security number, full name and/or data of birth and we obtain confirmation of information source name, address, and contact information.

Information is provided to employees responsible for such accuracy through various methods designed to train, educate, and remind them of these processes to ensure maximum possible accuracy of verification information. Such methods include but are not limited to:

1. Written Manuals
2. Online Manuals
3. Classroom Training
4. On the job training or training from an expert to provide assistance when needed

SafestHires, Inc

Policy: Current Employment Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires Inc is hereinafter referred to as "the company".

Overview

It is important when preparing consumer reports for employment screening purposes that the consumer reporting agency follow procedures to contact consumer's current employer only when authorized by the consumer or when the customer receives authorization from the consumer and provides such authorization to the consumer reporting agency.

Purpose

To avoid unnecessary risk, it is essential that contacts are only made with current employers when and if the consumer submits authorization to do so. There is a potential for a negative impact on the consumer if a current employer is contacted in conjunction with a consumer report for employment, especially when the current employer is unaware or does not approve of the consumer's job seeking activities.

Scope

This policy includes all employees that process and prepare consumer reports.

Policy

The company prohibits the contact with a consumer's current employer unless directly authorized by the customer and/or consumer. An authorization in writing either provided as a separate document or on the employment application signed by the consumer is required before any contact may be made. The company technology offers the ability to freeze the verification until the consumer authorizes the verification of current employment

The following methods are utilized to reasonable ensure the consumer's current employer is contacted only with authorization:

1. Authorization is provided on the employment application,
2. Explicit authorization is provided within the Disclosure/Authorization, signed by the consumer,
3. System technology will freeze or put the verification to a pending status until consumer provides authorization to verify current employment.

Employees are provided with adequate training on securing employment verifications including this policy on current employer verifications. Employees are instructed on the methods of securing consumer authorizations through the following:

1. Written materials/instructions
2. Online manuals or instructions
3. Classroom trainings

4. On the job education and availability of a more experienced employee when needed. Written materials are provided in all classrooms and on the job trainings.

SafestHires, Inc.

Policy: Accredited Academic Institutions Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to identify when post-secondary academic institutions are not accredited by and accrediting body recognized by U.S. Department of Education, Council of Higher Education Accreditation (CHEA), similar U.S. body, or comparable global body if reasonably available for academic institutions outside of the U.S.

Purpose

To avoid unnecessary risk and to ensure accuracy and credibility of reporting, it is important to know when post-secondary institutions are not properly accredited by accrediting bodies.

Scope

The scope of this policy includes all employees that process verifications.

Policy

The company maintains procedures through its relationship with the National Student Clearinghouse to identify when post-secondary academic institutions are not accredited by an accrediting body recognized by U.S. Department of Education, Council of Higher Education Accreditation (CHEA), similar U.S. body, or comparable global body, if reasonably available, for academic institutions outside the U.S.

We have and use methods to reasonably ensure the legitimacy of academic credentials and accrediting body. They include, but are not limited to confirmation using:

1) U.S. Department of Education,
2) the Council for Higher Education Accreditation,
3) state education departments,
4) similar U.S. body, and/or comparable global body, if reasonably available, for academic institutions outside the U.S.
5) National Student Clearinghouse

We have documented, in writing, our procedures used to determine whether the post-secondary academic institution is accredited by an accrediting body recognized by U.S. Department of Education, CHEA, or similar body and how we inform the customer which includes a notice on the verification report itself.

We provide information regarding verification of accreditation status of post-secondary academic institutions to our workers who are responsible for such verification by using various methods which may include, but are not limited to:

Written manuals,
Online manuals or instructions,
Classroom training,
On-the-job training, and/or availability of expert to aid when needed. If classroom or on-the-job training is used, a training outline or manual is used.

SafestHires, Inc

Policy: Procedural Disclosures Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employee
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

It is important for consumer reporting agencies to provide full disclosure to customers about general business practices regarding the number of attempts made to verify information, what constitutes an "attempt", locate fees, fees charged by the employer or service provider and standard question formats prior to providing verification products and services.

Purpose

To avoid unnecessary risk, it is essential that disclosure be made to customers outlining certain business practices pertaining to verification services including the number of attempts made, definition of attempt, affiliated fees, and formats. This sets proper expectations with customers and leaves nothing open for mis interpretation during the customer relationship.

Scope

The scope of this policy includes all employees.

Policy

The company provides all customers with written information regarding general verification business practices. These practices are provided to customers through written product descriptions, statement of work documents, written agreements and details within the verification report itself.

The Information provided to customer includes but is not limited to the following on verification services:

1. The number of attempts made by the company to verify information
2. What constitutes or defines an "attempt"
3. Fee charged by the employer of service provider, and
4. Standard question formats

5.5 Verification Databases - Affidavit

SafestHires, Inc does not compile, maintain files and the then resell employment or education information.

Name: Andrew Andersen

Title: Partner

Signature: _____

Date: _____

5.5 Use of Stored Data

SafestHires, Inc does not provide investigative consumer reports from stored data.

Name: Andrew Andersen

Title: Partner

Signature: _____

Date: _____

SafestHires, Inc.

Policy: Documentation of Verification Attempts Policy	Created: 5/18/2010
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires Inc is hereinafter referred to as "the company".

Overview

It is important for consumer reporting agencies to fully document all verification attempts and results of each attempt.

Purpose

To avoid unnecessary risk, it is essential that during every verification all attempts be recorded along with the results of each attempt.

Scope

The scope of this policy includes all employees preparing consumer reports particularly those processing verifications and employees responsible for writing training materials.

Policy

For every verification, we record the attempts made and results of each attempt. Specifically, the information we record includes, but is not limited to the:

1) date and time of contact or attempted contact,
2) method of contact (such as phone number dialed, fax number used, email address used, address to which information was mailed, etc.),
3) name and title of contact,
4) results of the attempt, and
5) the employee who made the attempt or obtained information

We have documented, in writing, our policy and procedures used to ensure that all attempts made to verify information are fully documented.

Employees who are tasked with securing verification information are provided with adequate training on obtaining, documenting, and reporting this information. Employees are instructed on the confirmation processes to assure maximum possible accuracy and provided resources in the form of:

1. Written materials/instructions
2. Online manuals or instructions
3. Classroom trainings
4. On the job education and availability of a more experienced employee when needed. Written materials are provided in all classrooms and on the job trainings.

SafestHires, Inc.

Policy: Outsourced Verification Services Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as “the company”.

Overview

As a consumer reporting agency, it is important to require a signed agreement from all providers of outsourced verification services. The agreement must describe the scope of services to be provided, the verification methodology, documentation of efforts to secure information, disclosure of findings, time frame for communication and completion of results, confidentiality requirements, reinvestigation requirements and other obligations as furnishers of information under the federal Fair Credit Reporting Act.

Purpose

To avoid unnecessary risk, it is necessary that all providers of outsourced verification information be under contract to fulfill certain obligations before providing information.

Scope

The scope of this policy includes all employees responsible for managing third party service provider relationships.

Policy

The company requires a signed agreement from any outsourced verification service utilized. The agreement must be signed by an authorized representative of the verifications firm prior to the firm performing any verification on our behalf. The agreement is required to contain the following stipulations:

1) the requirement to conduct all verifications in full compliance with applicable law and regulation,
2) scope of services provided,
3) methods used to obtain information,
4) time frame for communication and completion of requests,
5) methodology for confirming identity of subject of verification,
6) confidentiality requirements,
7) reinvestigation requirements,
8) documented "attempts to verify" per Clause 5.4,
9) background check requirements and acceptable results for provider's employees, and
10) signed non-disclosure agreements from provider's employees. Our agreements emphasize confidentiality requirements including:
A) the legal requirement to treat all consumer information as confidential,

B) secure data transmission, and
C) secure and timely disposal of confidential information.

We retain this agreement during the relationship and for a minimum of three years after the termination of service.

Provider Agreement for Service

(Verification Vendors)

I _____ of _____ hereby desire to perform services for SafestHires, Inc. agree to the following:

An outsourced Provider of Employment Verification, Employment Reference, or Educational Verification ("The Provider" as used herein) should take reasonable steps to accomplish the following, and should maintain documentation and a written audit trail for each step:

1) The Provider should take measures to ensure the "greatest possible accuracy" in obtaining information, including periodic audits of call histories and results designed to limit the possibility of clerical error.

2) The Provider should take appropriate measures to require sufficient data about the applicant and their past employer and/or educational institution, to ensure that there are no delays or inaccuracies caused by lack of sufficient details. The details should minimally include the full name of the applicant, any previous names if applicable, the name of the school or employer with the city and state, along with the information to be verified.

3) The Provider should have a procedure in place to ensure that a current employer is not contacted unless there is authorization from applicant. The Providers must recognize that contacting a current employer without the applicant's express consent can endanger the applicant's current job, and potentially cause liability to SafestHires, Inc or the Provider.

4) The Provider should take reasonable steps to prevent fraudulent verifications and references, including procedures to verify the identity and phone number of past employers and training of researchers in fraud detection.

5) The Provider should take reasonable steps to prevent fraudulent educational claims, including but not limited to identifying diploma mills and fake schools. In the event a diploma or degree is supplied by an applicant, to verify education, a best practice is to fax a copy of the document to the institution in question to determine authenticity.

6) The Provider should train and supervise all researchers to ensure all information is obtained in a professional and accurate manner.

7) The Provider should take reasonable steps to engage in a program to continually monitor adherence to these standards and to improve quality of services to these standards.

8) The Provider should have uniform procedures across all researchers including, but not limited to, rules setting forth the number of attempts made to complete a verification or verification of reference, what constitutes an attempt, procedures to locate schools or employers, and standard question formats.

Legal Compliance

9) The Provider must obtain from past employers only information that is permissible under state and federal law. The Provider should not ask any questions of past or current employers that would violate

generally accepted standards under federal and state EEOC rules, including but not limited to questions that identify a person on a basis covered by a discriminating law, or result in the disproportionate screening out of members of a protected group or are not valid predictors (not a job-related inquiry) of successful job performance. Prohibited inquiries include questions that in any way limit a person's job opportunities due to race, color, religion, national origin, ancestry, medical condition, disability (including AIDS), marital status, sex (including pregnancy), age (40+), exercise of family care leave or leave for an employee's own serious health condition.

10) The Provider must comply with FCRA section 614, and not use adverse information in its file that is older than 90 days that is not re-verified.

11) The Provider must follow the requirements of FCRA section 606(d)(4) concerning adverse information.

12) The Provider must comply with the Federal Family Educational rights and Privacy Act (FERPA) when obtaining educational verification.

13) The Provider must comply with all applicable labor laws governing individuals who are providing verification services.

Timeliness

14) The Provider should complete the majority of all orders within 72 hours from receipt of the order, and have the ability to track at any time any order that is older than 72 hours. Any order older than 72 hours should contain appropriate call history to indicate why that order took longer than 72 hours.

Performing the Search

15) The Provider should minimally make one solid attempt per day to contact the employer or school. A solid attempt does not mean a busy signal, incomplete call or some other act that is not reasonably likely to lead to the completion of the assignment of the order.

16) Provider should maintain a call history as defined above.

17) All employment and education verifications should be conducted in a physical environment where standards concerning privacy protection; computer and information security, training; supervision; quality control; safety of data and password integrity can be maintained across all work provided by the Provider.

Reporting the Search

18) Provider must accurately convey all information obtained during the course of the verification or reference to SafestHires, Inc.

19) In the event some information is not available, the Provider should indicate in the call history what steps were taken to obtain the information.

Correcting Information

20) The Provider should notify SafestHires, Inc immediately upon the discovery of any significant error or omission in the research.

21) Should an applicant dispute the results of a search, the Provider must regard the matter as a high priority and give their best effort to verify or correct the information disputed and should furthermore regard any such additional research as part of the original verification request as they were given to perform.

Audits

22) The Provider should maintain a complete history of all transactions, including the dates, times and results of all calls and the researcher who made each call for a period of six years. This is based upon a five year statute of limitations as defined by the FCRA (as amended in November 2004), plus an additional year to reflect the time that is typically allowed for service of process in the event of a lawsuit.

23) The Provider should recognize that SafestHires, Inc has a right to audit you by periodically submitting, unannounced, requests on an applicant with known results.

Confidentiality

24) The researcher must use reasonable procedures to maintain confidentiality of all information about an applicant, including but not limited to personal identifiable information.

25) All researchers must be trained on the need for confidentiality and sign confidentiality agreements with their employer.

26) The Provider of these services must not send personal identifiable information off-shore to be processed by researchers who are not subject to U.S. or Canadian Privacy laws.

Outline the scope of services to be provided to SafestHires, Inc.

_____
_____
_____
_____

Indicate the methods used to obtain information:

_____
_____
_____

All employees that will have access to a consumers personal identifiers information are required to have a background check (with acceptable results)

I certify I will utilize document disposal and/or destruction methods that shall render all disposed data unintelligible.

I agree to maintain all required licensure in my specific jurisdiction.

At no time shall this agreement constitute a contract for employment purposes. Each of the parties to the Agreement are independent contractors and nothing contained in this Agreement shall be construed as creating a joint venture, partnership, licensor-licensee, principle-agent, mutual agency relationship or employment agreement between or among the parties.

I understand that no changes in these conditions may be made except by consent in writing of an officer of SafestHires, Inc, Inc.

Provider:

Signed By: _____

Print Name: _____

Title: _____

Company Name: _____

Date: _____

SafestHires, Inc

Signed By: _____

Print Name: _____

Title: _____

SafestHires, Inc.

Policy: Conflicting Data Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires Inc is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to notify customers of conflicting data. Specifically in circumstances involving receipt of additional information or information after the delivery of the consumer report and as a direct result of the initial inquiry, that conflicts between the originally reported information and the new information received within 120 days of the initial report, a notification is necessary.

Purpose

To avoid unnecessary risk and ensure accuracy in the company reporting, it is essential to follow procedures to notify customers of conflicting data after the delivery of the initial consumer report.

Scope

The scope of this policy includes all employees.

Policy

Should the company receive information from the verification source subsequent to the delivery of the consumer report, and as a direct result of the initial inquiry, that conflicts with originally reported information, and that new information is received within 120 days of the initial report, (or as may be required by law), the company notifies the customer of such information.

If we receive information from the verification source after the delivery of the verification, and as a direct result of the original that conflicts with what we originally reported, we notify the client if the conflicting information was received within 120 days of the original. Specifically, we provide:

1) confirmation that conflicting information is specifically related to same consumer, same customer, and original report,

2) verification of the authenticity of the conflicting information and its source,

3) method used to update report,

4) method used to provide updated information to consumer and customer, and

5) the form in which the update is provided.

We have documented, in writing, our policy and procedures on how we handle conflicting data that has been received within 120 days and is a direct result of the original inquiry and how we then provide that information to the customer who originally ordered the report.

We provide information regarding processing and reporting of conflicting data to our employees who have this responsibility by using various methods which include, but are not limited to:

Written manuals,
Online manuals or instructions,
Classroom training,
On-the-job training, and/or availability of expert to provide assistance when needed. When classroom or on-the-job training is used, a training outline or manual is used.

SafestHires, Inc.

Policy: Authorized Recipient Policy	Created: 5/18/2021
Revisions: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires Inc is hereinafter referred to as “the company”.

Overview

As a consumer reporting agency, it is important to confirm that all verification requests are directed to authorized recipients. When making verification requests either by phone, fax, email or postal mail all requests must be delivered to an authorized party.

Purpose

To avoid unnecessary risk and to ensure maximum possible accuracy, all verification requests must be directed to an authorized party regardless of whether they are made through phone, fax, email, or postal mail.

Policy

The company utilizes methods to reasonably ensure that all verification requests are directed to an authorized recipient when requesting by phone, fax, email, or postal mail. Our methods include:

1. Confirming method used by information source to provide verification information,
2. Confirming company/institution name and address matches that provided by consumer, and
3. Obtaining name and title of person to whom request will be sent.

Employees who are tasked with securing verification information are provided with adequate training on obtaining, documenting, and reporting this information. Employees are instructed on the confirmation processes to assure maximum possible accuracy and provided resources in the form of:

1. Written materials/instructions
2. Online manuals or instructions
3. Classroom trainings
4. On the job education and availability of a more experienced employee when needed. Written materials are provided in all classrooms and on the job trainings.

SafestHires, Inc.

Policy: Background Check Policy on Company Owners	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to require criminal background checks and government sponsored sanction list checks be conducted on all company owners, officers, principals and those charged with enforcement of company policy. Checks must be conducted at official, appropriate government repositories to cover 7 years of residential history and such records must be retained unless otherwise prohibited by applicable law. Such record checks must be conducted at least every two years and records retained as long as the employee provides services to the company. Any criminal conviction(s) or sanctions listing(s) must be evaluated to determine if the individual may remain in his/her current position with the company based on 1) the nature and gravity of the offense or conduct, 2) time passed since the offense or completion of sentence and 3) the nature of current or desired role.

Purpose

To avoid unnecessary risk, it is essential that appropriate, reasonable and regular criminal background checks and sponsored sanction list checks be conducted on persons of influence within the company.

Scope

The scope of this policy includes Human Resources.

Policy

The company requires criminal background checks and government sponsored sanction list checks be conducted on all company owners, officers, principal's and those charged with enforcement of company policy. Checks must be conducted at official, appropriate government repositories to cover 7 years of residential history and such records must be retained unless otherwise prohibited by applicable law. Record checks must be conducted at least once every two years covering the time period since the last check was completed and records retained for the duration of enforcement responsibility. Any criminal conviction(s) or sanctions listing(s) must be evaluated to determine if the individual may remain in an enforcement capacity based on: 1) nature and gravity of offense or conduct, 2) time passed since offense, conduct, or completion of sentence and 3) nature of current enforcement role (commonly referred to as "Green Factors")

Record checks are conducted at least once every two years covering the time period since the last check was completed and records retained for the duration of enforcement responsibility. Any criminal conviction(s) or sanctions listing(s) are evaluated to determine if the individual may remain in an enforcement capacity based on: 1) nature and gravity of offense or conduct,

2) time passed since offense, conduct, or completion of sentence and

3) nature of current enforcement role (commonly referred to as “Green Factors”).

SafestHires, Inc.

Policy: Employee Background Check Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to require criminal background checks and government sponsored sanction list checks be conducted on all company employees. Checks must be conducted at official, appropriate government repositories to cover 7 years of residential history and such records must be retained unless otherwise prohibited by applicable law. Such record checks must be conducted at least every two years and records retained as long as the employee provides services to the company. Any criminal conviction(s) or sanctions listing(s) must be evaluated to determine if the individual may remain in his/her current position with the company based on 1) the nature and gravity of the offense or conduct, 2) time passed since the offense or completion of sentence and 3) the nature of current or desired role.

Purpose

To avoid unnecessary risk and to ensure that employees performing services for the company are reviewed routinely for criminal convictions or sanctions and that any employee found to have either a criminal conviction or sanction be evaluated to determine if they may remain in their position based on the nature and gravity of the offense, time elapsed and the nature of the employee's role.

Scope

The scope of this policy includes Human Resources.

Policy

The company requires criminal background checks and government sponsored sanction list checks be conducted on all employees. Checks must be conducted at official, appropriate government repositories to cover 7 years of residential history and such records must be retained unless otherwise prohibited by applicable law. Record checks must be conducted at least once every two years covering the time period since the last check was completed and records retained for the duration of employment with the company. Any criminal conviction(s) or sanctions listing(s) must be evaluated to determine if the individual may remain employed with the company based on: 1) nature and gravity of offense or conduct, 2) time passed since offense, conduct, or completion of sentence and 3) nature of current enforcement role (commonly referred to as "Green Factors")

Record checks are conducted at least once every two years covering the time period since the last check was completed and records retained for the duration of employment with the company.

Any criminal conviction(s) or sanctions listing(s) are evaluated to determine if the individual may remain employed with the company based on:

1) nature and gravity of offense or conduct,

2) time passed since offense, conduct, or completion of sentence and

3) nature of current enforcement role (commonly referred to as “Green Factors”).

SafestHires, Inc.

Policy: Customer Authentication Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

It is important to identify and authenticate all customers prior to disclosing consumer information. As a consumer reporting agency written records must be maintained regarding the qualification of every customer who receives consumer reports or other consumer information.

Purpose

To avoid unnecessary risk, it is essential that customers be authenticated before disclosing consumer information.

Scope

The scope of this policy includes employees responsible for credentialing customers.

Policy

The company requires that prior to providing any consumer information, due diligence is performed to authenticate customers. The procedure requires written records regarding the qualification of each customer who receives consumer reports or other consumer information be maintained.

Before providing any consumer information, we are to perform due diligence to authenticate the customer. Specifically, our authentication methods include, but are not limited to:

Obtaining evidence of right to conduct business, such as copy of business license, articles of incorporation or state filing etc., and authentication thereof,

1. PHONE NUMBER VERIFICATION
2. WEBSITE VERIFICATION
3. EXPORT.COM AND OFAC
4. PROOF OF BONA FIDE ENTITY
5. BUSINESS CREDIT REPORT
6. EXPERIAN END-USER ALERT LIST
7. EQUIFAX AND TRANSUNION ALERT LIST
8. FDIC AND NCUA (if applicable)

And may include a PHYSICAL INSPECTION

SafestHires, Inc.

Policy: Vendor Authentication Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as "the company".

Overview

It is important to identify and authenticate all vendors prior to disclosing consumer information. As a consumer reporting agency written records must be maintained regarding the qualification of every vendor who receives consumer information.

Purpose

To avoid unnecessary risk, it is essential that vendors be authenticated before disclosing consumer information.

Scope

The scope of this policy includes employees responsible for credentialing vendors.

Policy

The company requires that prior to providing any consumer information, due diligence is performed to authenticate vendors.

For vendors which are nationally recognized and commonly used by the background screening industry, a signed agreement with the vendor serves as authentication. Examples of these vendors include the three national credit bureaus, repositories of education and employment data and motor vehicle record resellers.

For unknown vendors, authentication records must include but are not limited to:
1. Obtaining evidence of right to conduct business, such as a copy of a business license, articles of incorporation or state filing and authentication thereof,
2. Verification of a working business phone, fax, email and website,
3. Reference through a minimum of one independent third-party, and
4. Previous work experience and/or onsite inspection results.

SafestHires, Inc.

Policy: Consumer Authentication Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

Operating as a consumer reporting agency, it is important to obtain proof of consumer identity before providing any information to a consumer making a telephone inquiry. It is critical to document the information used to identify each consumer to whom consumer information is being provided.

Purpose

To avoid unnecessary risk and to avoid providing information from fraudulent requests from consumers, the consumer be adequately authenticated as legitimate prior to releasing information to telephone inquiries.

Scope

The scope of this policy includes all employees.

Policy

Prior to releasing information to a consumer with a telephone inquiry, the following identification/authentication questions are asked of the consumer. Confirmation of full name as provided on the consumer report must be provided along with at least two of the following personal identification items:

1. Date of Birth
2. Street address used on application or authorization document
3. Last four digits of SSN/Country ID
4. Drivers License Number
5. Report ID Number

The company retains a record of the information used to identify and authenticate the consumer.

SafestHires, Inc.

Policy: Record Retention Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to maintain complaint practices for record retention and data destruction. Record retention and data destruction procedures must comply with all applicable law and regulation.

Purpose

To avoid unnecessary risk, it is important that consumer sensitive information be retained for the correct amount of time and that consumer sensitive information be disposed of through methods compliant with all applicable law and regulation including but not limited to the federal Fair Credit Reporting Act.

Scope

The scope of this policy includes all employees of the company.

Policy

The company record retention and destruction for consumer records processes address both electronic and hard copy (paper) records and include:

1) the period of retention for consumer records
2) method used to determine record age
3) processes used for actual record destruction
4) documentation of record destruction activity, and
5) individual responsible for initiating, managing, confirming and documenting record destruction.

All consumer records are maintained for a minimum of 2 years and destroy consumer records after 7 years. Exceptions to this rule are records involved in litigation or investigation by a government agency, or advice of legal counsel.

Hard Copy Destruction

While the Company standard is not to have consumer information on hard copies, any papers containing consumer information are shredded so information cannot be read or reconstructed. Shredding logs are maintained.

Electronic Destruction

A commercial grade program is used to destroy/erase electronic files or media containing consumer information so that information cannot be read or reconstructed. Destruction logs are maintained.

Mark Colbath is the company designated party responsible for initiating, managing, confirming, and documenting all record destruction.

SafestHires, Inc.

Policy: Employee Certification Requirement Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to require employees to certify in writing they will adhere to the confidentiality, security, and legal compliance practices of the company to ensure 100 percent compliance.

Purpose

It is important that prior to beginning employment duties, all new hires to the company certify in writing they will comply with all company practices regarding confidentiality, data security and legal compliance requirements. This will help to reduce overall risk to the company and help to ensure employees are performing in a compliant manner regarding confidentiality, security, and legal compliance.

Scope

The scope of this policy includes all employees and Human Resources.

Policy

The company requires that all employees certify in writing at time of hire before they begin their employment duties, they will adhere to all company policies and practices regarding confidentiality, data security, and legal compliance. Current workers hired before the implementation of this policy are required to retroactively certify their adherence. Certifications for all employees are retained in employee files maintained by the company.

SafestHires, Inc.

Policy: Employee Certification Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to provide initial and ongoing training to employees where training is commensurate with specific worker roles and responsibilities. Equally as important is to provide training on overall, general requirements on confidentiality, professionalism, accuracy, and employee's role as a representative of a consumer reporting association. Training shall be provided prior to assuming the employee role and then continue throughout employment with the CRA. Records of all trainings shall be retained.

Purpose

To avoid unnecessary risk, it is essential that employees be given adequate training before they assume their duties and then ongoing training afterwards. Training should be both specific to worker roles and responsibilities and more generalized on confidentiality, professionalism, and accuracy.

Scope

The scope of this policy includes Human Resources and all employees.

Policy

The company training program is patterned after the US Navy Personnel Standards Qualification Program (PQS). Use of PQS provides a trainee with references, theory, and practical application necessary to learn and perform specific duties. PQS qualifiers are Senior Account Executives and Account Supervisors who have satisfied the PQS requirements for their position and satisfactorily performed these duties for at least one year. Our PQS program is divided into three Phases.

The Fundamentals Phase presents the fundamental knowledge from Senior Account Executive input necessary to satisfactorily understand the position duties. - One week.

The Systems Phase is designed to acquaint the employee with the systems they will be required to operate and processes they will be required to follow. This is all hands-on supervisor training - One week.

The Performance Phase lists the tasks the employee will be required to satisfactorily perform in order to achieve final PQS qualification for their position. This is monitored by supervisors. - Two weeks.

In order to complete each Phase, the trainee must satisfactorily answer a series of questions from supervisors related to the position (and in the final phase, perform certain functions) relevant to that

Phase. Once all questions have been correctly answered, the trainee “shadows” the qualifier in performing their duties for 90 days.

Employees are provided with ongoing training throughout employment with the company. Employees are provided resources in the form of:

1. Written materials/instructions
2. Online manuals or instructions
3. Classroom trainings4. On the job education and availability of a more experienced employee when needed. Written materials are provided in all classrooms and on the job trainings.

All training material is documented, and evidence of employee trainings are maintained by the company.

SafestHires, Inc.

Policy: Employee Certification Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

Operating as a consumer reporting agency, it is important to provide employees with initial and annual training on confidentiality, security, and legal compliance practices and to maintain records of such trainings.

Purpose

To avoid unnecessary risk and to ensure employees are adequately trained on industry important topic such as confidentiality, security, and legal compliance, it is essential that all employees be provided with education at the start of their employment and annually thereafter.

Scope

The scope of this policy includes all employees.

Policy

The company provides training to all employees both at time of hire and annually thereafter on such topics as confidentiality, data security and legal compliance practices. All employees are required to participate in these trainings. These trainings are required before new hires to the company assume their duties and responsibilities.

Training methods includes on or more of the following but are not limited to:

1. Written Material
2. Online Training
3. Training Classes/Webinars
4. One on One Training Sessions
5. On the Job Training

Participation records are maintained to show evidence of all employee trainings.

Confidentiality, data security and legal and compliance is referred to in the company employee handbook. All employee requirements concerning confidentiality, data security and legal compliance are documented in writing and reviewed during all training events within the company.

SafestHires, Inc.

Policy: Visitor Security Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to ensure that visitors do not view or have access to consumer information.

Purpose

To avoid unnecessary risk, reasonable procedures need to be followed to ensure that visitors are protected from viewing or accessing consumer information.

Scope

The scope of this policy includes all employees.

Policy

The company maintains a visitor security program to ensure visitors do not view or have access to consumer information. We ensure that visitors are prevented from viewing or accessing consumer information. Specifically, these methods may include, but are not limited to:

Use of sign in/out registry,

Issuance of temporary badges,

Situations in which a Company employee must escort the visitor,

Controlled access to systems and data, and

Controlled access to areas of facility in which consumer information is readily available on screens or hard copy.

For Non-Employees, access to the building is limited to the front door during regular business hours of operation. All visitors must register at the front desk by signing their name and the individual with whom they will visit. All Non-Employees must have proper identification be escorted by a company employee at all times while visiting.

SafestHires, Inc.

Policy: Responsible Party Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc. is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to designate one individual to oversee and administer the accreditation process and ongoing compliance including the enforcement of the Accreditation Standard. The dedicated party must be vested with the responsibilities and authority to fulfill this role and must be the contact for the PBSA Auditor and all accreditation related matters.

Purpose

It is important to have one designated contact for the accreditation process and ongoing compliance matters.

Scope

This policy includes the designated individual who will oversee and administer the accreditation process and ongoing compliance.

Policy

The company designates Andrew Andersen as its designated individual to oversee and administer the accreditation process and ongoing compliance including the enforcement of the Accreditation Standards. Andrew Andersen is vested with the responsibilities and has the authority to fulfill this role and will be the contact for PBSA and its auditor for all accreditation related matters. Andrew Andersen has provided a signed affidavit in which he affirms responsibility for accreditation and future compliance and that he is qualified to hold this responsibility.

SafestHires, Inc.

Policy: Document Control Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

As a consumer reporting agency, it is important to maintain procedures for document control and versioning to ensure correct versions of all controlled documents are being used.

Purpose

To avoid unnecessary risk, including the risk of using older versions of various policies, it is important to maintain a system of version control.

Scope

This policy includes employees responsible for writing and approving policies and policy revisions.

Policy

The company is committed to ensuring that documents used internally and externally are approved by management and cannot be edited without permission, are readily accessible and identifiable as the most recent version or an archived version. The company reviews policy and procedures annually to ensure the currency of these documents.

Training is provided to ensure employees are knowledgeable on how to retrieve and use only the most current version of any controlled document. We use one or more methods which include but are not limited to 1) user manual/guide, 2) online training, user guides or help system, 3) user training classes/webinars, 4) one-on-one training sessions, or 5) verbal assistance.

The company Document Control Policy documents procedures on how we:

1) approve documents for adequacy prior to issue,
2) review, update as necessary, and re-approve documents,
3) identify the changes and current document revision status,
4) make relevant documents available at points of use,
5) ensure the documents remain legible and readily identifiable,
6) identify external documents and control their distribution,
7) prevent obsolete documents from unintended use,
8) apply suitable identification if obsolete documents are retained,
9) train employees and document the training

Document Control Policy and Procedures

Approving documents for adequacy prior to issue
Any document that is provided to customers or prospects must be approved. These controlled documents include but are not limited to:

Agreements, user guides, user training materials, sales materials, pricing sheets, required notices and brochures.

Any document that is used during business by employees that instructs them on how to perform their work duties. These controlled documents include but are not limited to:

SOPs, criminal record reporting guidelines, Policies and Procedures, Employee Handbook and training materials.

When any controlled documents listed above are created or amended, the manager of the document area recommends the addition or change to Andrew Andersen and only Andrew can approve the document or change and insert the document into the working drive for reference by all employees.

All policies are reviewed annually by Andrew Andersen and reviewed/revision dates are noted on the policy.

Reviewing, Updating as Necessary and Re-Approving Documents

Documents maybe reviewed and updated in the normal course of business. New federal or state laws or regulations as well as changing best practices from counsel necessitate change recommendations throughout the year.
In addition managers review documents in their working group annually to ensure working documents are accurate, relevant, and most up to date. Any deficiencies or needed additions will be recommended to Andrew Andersen.

Identifying the Changes and Current Document Revision Status

For each change made to an existing controlled document, a brief note of the changes made along with the month/year is noted.

Revision status is the version to be noted in the heading of the document. Example:
Revision Date 2-2020, A Year later the Revision Date would change to 2-2021

Making Relevant Documents Available at Points of Use

Documents must be available to the employees and manager when they are needed. To this end, all relevant, controlled documents are made available to employees who receive instructions on how to receive them.

Ensuring the Documents Remain Legible and Readily Available

Documents are stored in .pdf format. All documents are titled to reflect the document's content.

Identifying External Documents and Controlling their Distribution

Documents that are sent outside of the company are identified and controlled. Examples of external documents that must be identified include but are not limited to:
Agreements, user guides, user training materials, sales materials, price lists, required notices and brochures

Preventing Obsolete Documents from Unintended Use

Obsolete information is deleted or clearly marked as "OLD". Upon the revision of a document, or the creation of a new document that supersedes an existing document (or documents) the earlier version or obsolete documents are moved to an archive folder if they are not deleted entirely.

Apply Suitable Identification if Obsolete Documents are Retained

There are circumstances in which old documents are not current but valuable for reference or for building upon. For example, a webinar given two years ago may not be current, but the template and some slides may remain of value. To ensure obsolete documents are not used as current, they are moved to separate folders or marked as "OLD".

Training Employees and Documenting the Training

Training of employees on this policy including the identification, retrieval, and u se of only the most current version of any controlled document is a part of every employee's initial training. This is conducted by the employee's supervisor or manager.

Relevant documents are available at all points of use. Documents are legible and readily identifiable.

Records are retained of participants in these trainings.

SafestHires, Inc.

Policy: Ethics Reporting Policy	Created: 5/18/2021
Revision: 5/18/2021	Target Audience: All Employees
Responsible Party: Andrew Andersen	CONFIDENTIAL

SafestHires, Inc is hereinafter referred to as "the company".

Overview

It is important that employees have a process whereby they can anonymously, to the extent possible, report ethical, compliance, and work product concerns without fear of identification or retaliation based on such reporting. Such processes must include the communicating to employees the vehicle(s) by which they may report with anonymity. Procedures for investigation of reported concerns must also be in place to manage and respond to employee reports.

Purpose

It is important that employees have a process to report anonymously any concerns regarding ethical, compliance and work product concerns without fear of identification or retaliation.

Scope

The scope of this policy includes all employees.

Policy

The company is committed to the highest levels of ethical, compliance and work product standards.

There are procedures whereby employees may anonymously, to the extent possible, report any ethical, compliance, and work product concerns without fear of identification or retaliation based on such reporting.

If for any reason any employee does not feel comfortable reporting with their supervisor or direct manager regarding ethical, compliance or work product concerns, the company has a process for such concerns to be reported to a designated individual who is tasked to investigate the matter while maintaining the anonymity of the reporting worker to the extent possible. In addition to the anonymity, we guarantee they will not be subject to any retaliation or adverse action based on their reporting. In the event the company designated liaison is unavailable, we have designated an alternative liaison who is educated and responsible to the same degree as the primary liaison.

Employees are educated on the availability and facts on this policy and procedure during their initial training and this information is also included in the company Employee Handbook.

The designated liaison for the company is Andrew Andersen and the alternative liaison recommended by Andrew on a case-by-case basis. The liaison(s) are available by telephone or email and both individuals understand the importance of anonymity.