PBSA BACKGROUND SCREENING ORGANIZATION ACCREDITATION PROGRAM – BSOAP GENERAL ACCREDITATION STANDARD AND AUDIT CRITERIA (Glossary provided at end of document.)

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit (What auditor will look for in policy, procedure, activity)
Information Security			
1.1 Information Security Certification			
Any system (i.e., platform, application, database) which is used to store and access Personally Identifiable Information (Personal Data), whether with the organization, and/or organization's platform provider (whether internal or hosted) must be within the scope of a current (current as defined by the certifying body) information security certification and/or provide written evidence of completing an information security audit for which no critical, high-risk, or severe security vulnerabilities remain uncured. The source of such certification and/or written evidence must be a qualified security assessor.	Any system (i.e., platform, application, database) which is used to store and access Personally Identifiable Information (Personal Data), whether with the organization, and/or organization's platform provider (whether internal or hosted) must be within the scope of a current (current as defined by the certifying body) information security certification or completion of information security audit for which no critical, high-risk, or severe security vulnerabilities remain uncured. Written evidence must include name of security standard used as basis for auditing and at least one of the following from a qualified security assessor: 1) certification document, 2) audit results signed by 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 statement that no critical, high-risk, or severe security vulnerabilities were found or, if found, such vulnerabilities have been cured.	Organization, and/or organization's platform provider (whether internal or hosted) must provide evidence from a qualified security assessor of current information security certification or completion of information security audit for which no critical, high-risk, or severe security vulnerabilities remain uncured.	Any system (i.e., platform, application, database) which is used to store and access Personal Data, whether with the organization, and/or organization's platform provider (whether internal or hosted) must be within the scope of a current (current as defined by the certifying body) information security certification or written evidence of information security audit by a qualified security assessor for which no critical, high-risk, or severe security vulnerabilities remain uncured. Written evidence of audits will be acceptable if: 1) certification document is provided, 2) audit results signed by auditor show no critical, high-risk, or severe security vulnerabilities remain uncured, or 3) signed attestation from auditor including date of audit, name of qualified security assessor, name of auditing company, statement that no critical, high-risk, or critical security vulnerabilities remain uncured, and 4) name of security standard(s) used as basis for auditing.
1.2 Information Security Policy			
Organization must have and follow a written information security policy which, at a minimum, complies with applicable law and regulation. Organization must designate one or more individuals responsible for implementing, managing and enforcing the information security policy (individual(s) may be internal or contracted.)	Organization must provide written information security policy.	Organization must present written information security policy and provide evidence of adherence to such policy. If questioned, organization workers must demonstrate knowledge of information security policy and be able to access current policy.	This is an overarching information security policy which broadly addresses security within the organization environment. This policy may reference other security policies and/or procedures dealing with specific security topics. Such document(s) must, at a minimum, address: 1) key personnel, roles and responsibilities, 2) policy changes and modifications, 3) system configuration, 4) anti-virus, firewall, and router configuration, 5) data and information classification, 6) encryption, 7) access control, 8) electronic data retention, storage, and disposal, 9) paper and hard data retention, storage, and disposal, 10) data device retention, storage, and disposal, 11) incident response, 12) physical security, and 13) security policy revision history. Auditor will seek evidence of adherence to policy

1.2 Information Security Policy (continued)			
Designated individual must have the required authority and independence to fulfill their duties under this Clause. Designated individual must be insulated from adverse employment actions resulting from the competent execution of their duties.	Organization must employ or retain a minimum of one person who is responsible for organization's overall information security program. This must be evidenced by written job description, policy, procedure, executed agreement or other documentation. If various people are responsible for different aspects of the program, one person must hold overall responsibility as evidenced by job description, organizational chart, or other documentation.	Organization must present written job description, policy, procedure or other documentation which identifies, by name and title, the person responsible for the overall information security program. If questioned, organization workers must identify individual responsible for overall information security program.	Organization must present documentation which clearly identifies person, by name and title, responsible for overall information security program.
1.3 Data Security			
Organization must have and follow procedures to protect subject information under the control of the organization from internal and external unauthorized access. These procedures must 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. At a minimum, procedures must meet all applicable legal and regulatory requirements.	Organization must provide written procedures to protect subject information from unauthorized electronic and/or physical access. This includes the collection, use, storage, transmission, and destruction of subject information in both paper and electronic form.	Organization workers dealing with subject information must be able to explain and demonstrate procedures for protecting subject information in their possession, whether such information is used internally and/or externally, be able to access current documentation, and provide evidence of adherence to such procedures. Organization must also be able to demonstrate electronic and physical protection of subject information. Organization must provide evidence of adherence to such procedures.	The policies and procedures designed to protect subject information must include, but are not limited to, the following: 1) securing unattended workstations, 2) limiting access to networks, data, and work areas, 3) limiting subject information provided to information sources to only that information which is needed for a specific business purpose, 4) destruction of hard copy documents, 5) identification of caller before providing subject information, 6) organization worker badging or other identification system, 7) unescorted visitor policy, 8) secure document destruction, 9) secure transport of information, 10) use of encryption and/or secure networks and/or websites, 11) control of access to subject information, 12) controlling use of portable storage devices, 13) alarm systems, 14) door locks, and 15) secure server and back-up sites. Auditor will seek evidence of adherence to policies and procedures.
1.4 Intrusion, Data Breach, and Data Security Incidents			
Organization must have and follow procedures to detect, investigate, respond to and recover from an actual or suspected information system intrusion, and/or data breach, including subject and client notifications and other breach notifications where mandated. At a minimum, procedures must meet all applicable legal and regulatory requirements. In the event of a breach, an organization should have documented recovery/business resumption procedures.	Organization must provide procedures for preventing, detecting, identifying, and responding to information system intrusions (unauthorized access to computer systems and/or subject data) and data security breaches.	Organization must make available the procedure, process, and tools used to prevent unauthorized access, monitor access and identify potential intrusions; organization must provide evidence of adherence to such procedures.	Organization must present proof of tools used to protect network, data, and subject information. This may be third party audit results, intrusion/detection testing results, firewall protections used, website security, or other recognized security protocols and devices. Auditor will seek evidence of adherence to policies and procedures.
	Organization must provide procedures for responding to information system intrusions including how subject notification and other breach requirements are determined.	Organization must make available the procedure, process, and/or tools used to respond to intrusions. If questioned, organization workers must demonstrate knowledge of procedure to be followed in case of actual or suspected intrusion, data security breach and be able to access current documentation. Organization must provide evidence of adherence to such procedures.	Process/procedure must include, but is not limited to: 1) individual to contact in case of intrusion and his/her back-ups, 2) necessity of immediately stopping intrusion activity, if still occurring, 3) determination of notification requirements, 4) preparing notification(s), 5) obtaining necessary approvals of notification language, 6) communicating notification, and 7) de-brief to prevent future occurrences. Auditor will seek evidence of adherence to policies and procedures.

1.5 Storage and Backup of Data			
Organization must have and follow procedures to ensure data is backed up and stored in an encrypted or otherwise protected manner. At a minimum, procedures must meet all applicable legal and regulatory requirements.	Organization must provide written policy, procedure or other documentation explaining data backup, storage, and access procedures.	Organization must make available the procedure, process, and/or tools used to manage data backup and storage. Organization must make available the individual responsible for data backup and storage. This individual must be able to describe and provide documentation related to backup and data storage. Organization must provide evidence of adherence to procedures.	The process used to backup and store data must include, but is not limited to: 1) limiting access to backup data to select authorized individuals, 2) secure transport of backup data to storage location (including virtual storage), and 3) security at the storage location. 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. Auditor will seek evidence of adherence to policies and procedures.
1.6 Access Protocol			
Organization must have and follow procedures requiring use of secure access protocols for organization workers, authorized client users, and any other authorized users accessing subject Information. At a minimum, procedures must meet all applicable legal and regulatory requirements.	Organization must provide written policy, procedure, or other documentation which explains access protocols for organization workers and authorized client users with access to subject information.	Organization must make available the individual responsible for access protocol. This individual must be able to describe and provide documentation related to access protocols including assignment, replacement, and recordkeeping. If questioned, organization workers with access to subject information must explain process to obtain access for him/her and/or authorized client users and be able to access current documentation. Organization must provide evidence of adherence to procedures.	Organization must demonstrate that access to subject information by organization workers and authorized client users is controlled. Acceptable access protocols may include, but are not limited to, strong passwords, biometric identification, and/or multi-factor identification. Records of access protocol issuance must be securely maintained. Auditor will seek evidence of adherence to policies and procedures.
1.7 Electronic Access Control			
Organization must have and follow procedures to control access to all electronic information systems and electronic media that contain subject information. Organization must have procedures in place to administer access rights. Organization workers and authorized client users must only be given the access necessary to perform their required functions. Access rights must be updated based on personnel or system changes.	Organization must provide written policy, procedure or other documentation explaining how access rights to subject information by organization workers and authorized client users are controlled and administered.	Organization must make available the individual responsible for controlling access to subject information. This individual must be able to describe and/or provide documentation and/or provide a demonstration related to access control. If questioned, organization workers who receive requests for access to subject information will demonstrate knowledge of process to add or change access rights for organization workers and authorized client users. organization must provide evidence of adherence to procedures.	Process must include, but is not limited to: 1) how organization workers and authorized client users apply for and receive access, 2) authorization needed for access, 3) access parameters, 4) issuance, replacement, and expiration of access rights, 5) monitoring tools, and 6) recordkeeping. Auditor will seek evidence of adherence to policies and procedures.

1.8 Physical Security			
Organization must have and follow procedures to control physical access to all areas of organization facilities, including data storage facilities that contain subject information.	Organization must provide written policy, procedure or other documentation explaining how access to areas of organization facilities containing subject information is controlled for organization workers, vendors, and guests and how records of such access are maintained.	Organization must provide auditor a tour of the facility, demonstrating and describing the physical security measures in place. Auditor may interview organization workers about physical security procedures and, if questioned, workers must describe physical security protocols and be able to access current documentation. Organization must provide evidence of adherence to procedures.	Process/procedure must cover organization workers, vendors, and guests, and include, but not be limited to, the following: 1) procedures for granting levels of access to organization workers (e.g., assignment of keys or security system passcodes), 2) procedures for authorizing and monitoring guests (including the auditor) to the facility, and 3) control of access by organization workers, vendors, and guests. Auditor will seek evidence of adherence to policies and procedures.
1.9 Subject Information Privacy Policy			
Organization must have and follow a subject Information Privacy Notice detailing the purpose of the collection of subject information, the intended use, and how the information will be shared, stored and destroyed and other requirements with applicable law. The organization must post this Notice on its website, if it has one, otherwise provide directly to clients. Organization must have and follow procedures to make said policy available to clients and/or subjects upon request and in at least one other format.	Organization must provide a copy of the subject Information Privacy Notice along with the address of the notice on the organization's website (if organization has website). Organization must provide written notice, procedure, or other documentation explaining other means by which privacy notice is requested and provided. Organization must provide written evidence, such as policies and procedures which demonstrate how the obligations contained in the privacy notice are met.	Organization workers must be able to access current copy of Privacy Notice and access current documentation describing process by which privacy notice is provided externally. Organization must provide evidence of adherence to procedures.	The notice must include, but is not limited to, the following: the purpose of the collection of subject information, the intended use, and how the information will be shared, stored and destroyed and any other requirements of applicable law. The organization must post this notice on its website, if it has one, and have procedure to make said notice available to clients and/or subjects upon request utilizing at least one other method. Auditor will seek evidence of adherence to policies and procedures.
1.10 Unauthorized Browsing			
Organization must have and follow a policy that prohibits organization workers from searching files and databases unless they have a bona fide business necessity.	Organization must provide written policy, procedure, or other document (organization worker handbook, etc.) which instructs organization workers on appropriate and/or inappropriate access and use of subject information.	Organization workers with access to subject information must demonstrate knowledge of proper access and use of subject information and be able to access current copy of documentation. Organization must provide evidence of adherence to procedures.	Documentation must include, but is not limited to, statement of appropriate use as being limited to business purposes only and include prohibition of browsing. Auditor will seek evidence of adherence to policies and procedures.
1.11 Record Destruction			
When records containing subject information are to be destroyed or disposed of, organization must have and follow a policy meeting all applicable legal and regulatory requirements, if such requirements exist, and ensure that all such records and data are destroyed and unrecoverable.	Organization must provide written policy, procedure, or other document (organization worker handbook, etc.) which instructs organization workers on appropriate document disposal and destruction procedures. If specific document destruction requirements exist, they shall be specified.	Organization workers must demonstrate knowledge and use of proper document disposal and destruction procedures and be able to access current documentation. Organization must provide evidence of adherence to procedures.	Documentation must require all subject and client information be destroyed and disposed of securely as to render information inaccessible, unreadable, and unrecoverable. The following methods are permitted: 1) burning, pulverizing, or shredding, 2) destroying or erasing electronic files, and/or 3) after conducting due diligence, hiring a document destruction company. In addition, paper documents containing personally identifiable information (particularly name, date of birth, and personal identification number), or sensitive information, as defined in that jurisdiction, if retained at individual desks/workstations, must be destroyed or inaccessible no later than the end of each work day/work shift. Auditor will seek evidence of adherence to policies and procedures.

1.12 Data Minimization			
Organization must have and follow a procedure to limit identifying data to only what is required to deliver a background screening service. This may include limits on required information or a process to suppress or truncate sensitive data elements. If client requires full sensitive data elements, organization must provide notification that client must comply with all applicable legal and regulatory requirements in regard to use, safeguarding, and destruction of such information.	Organization must provide written policy, procedure, or other documentation describing data minimization, suppression, truncation, or other methods used to protect and limit collection or exposure of personal identification numbers and other sensitive data elements as required by law or as agreed to with the client.	Organization workers must demonstrate knowledge of proper procedures for collection, use, and minimization of personal identification numbers, data and other sensitive data elements as required by law and organization workers shall be able to access current documentation. If interviewed, organization workers must demonstrate understanding of proper use and protection of sensitive data as required by law or as agreed to with the client AND if applicable, the use of technology to protect sensitive data elements as required by law. Organization must provide evidence of adherence to procedures.	Documentation must include but is not limited to: 1) No more than the four digits/characters of personal identification numbers shall be communicated in any form outside the organization environment unless an approved exception exists; 2) When use of personal identification number and other sensitive data elements as required by law or as agreed to with the client is needed internally or externally, the data exposed shall be limited to only that which is needed for the specific business purpose which has been identified; 3) When communicating personal identification numbers or other data, or necessary business purpose outside the organization environment, secure transport methods must be used. Auditor will seek evidence of adherence to policies and procedures.
Legal and Compliance			
2.1 Compliance with Law and Regulation			
The organization must comply with all provisions of all applicable law and regulation pertaining to the subject reports provided by the organization for background screening purposes.	Organization must provide written policy, procedure, or other documentation which clearly informs organization workers of requirement to comply with all applicable law and regulation.	Organization workers must demonstrate knowledge of compliance requirements and be able to access current copy of documentation. Organization workers must be able to identify person(s) responsible for legal and regulatory compliance. Organization must provide evidence of adherence to procedures.	Organization must provide documentation describing how organization workers are informed of compliance requirement and compliance leader(s). Methods to inform organization workers must include at least one of the following: 1) inclusion in organization Worker Handbook, 2) inclusion in organization worker employment agreement, or 3) inclusion in online document repository where organization operational policies and procedures are made available to organization workers. Auditor will seek evidence of adherence to policies and procedures.
2.2 Reporting Law			
The organization must designate an individual(s) or position(s) within the organization responsible for organization's compliance with all legal and privacy requirements that pertain to the reports provided by the organization for background screening purposes. Such positions may be Chief Compliance Officer, Privacy Officer, Operations Manager or General Counsel. Designated individual must have the required authority and independence to fulfill their duties under this Clause. Designated individual must be insulated from adverse employment actions resulting from their competent execution of their duties.	Organization must employ a minimum of one person who is responsible for organization's development, implementation, and on-going compliance with legal and privacy requirements as evidenced by written job description(s) or other documentation. If multiple people are responsible, one person must hold overall responsibility as evidenced by written job description or other documentation.	Organization must present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for legal and privacy compliance. Organization must provide evidence of the same. Organization must make this person available in person. If interviewed, organization workers must identify the person(s) that can provide legal and privacy expertise when needed.	Organization Compliance Leader must affirm his/her role as being responsible for legal and privacy compliance within the organization. Ideally this individual's contact information should be listed on the organization's online privacy notice.
Organization must have and follow procedures to forward privacy-related individual requests or complaints to the client or to handle them when instructed.	Organization must provide written policy, procedure, or other written documentation (such as organization worker handbook) clearly outlining the process for directing privacy related requests or complaints to the client when instructed.	Organization must present one or more documents which clearly outlining the process for directing privacy related requests or complaints to the client when instructed. If interviewed, organization workers responsible for handling such requests must demonstrate knowledge of and be able to access current documentation.	Provided documentation must include the process for directing privacy related requests or complaints to the client when instructed.

2.6 Integrity			
Organization must have and follow a policy of not engaging in bribery or any other unlawful activity to obtain preferential treatment from a public official or government entity.	Organization must provide written policy, procedure, or other written documentation (such as organization worker handbook) clearly prohibiting bribery or any other unlawful activity to obtain preferential treatment from a public official or government entity.	Organization must present one or more documents which clearly prohibit bribery or any other fraudulent activity to obtain preferential treatment from a public official or government entity. If interviewed, organization workers responsible for obtaining record information must demonstrate knowledge of anti-bribery/unlawful activity policy and be able to access current documentation. Organization must affirm that they do not engage in bribery or other fraudulent activity and that organization has never been convicted of such activity.	The policy must include, but is not limited to, a directive to all organization workers that there is a prohibition of bribery and any other fraudulent activity and an attestation by a senior member of the organization that it has not engaged in any bribery or other unlawful activity. If organization has disclosed activities of bribery or other unlawful activity, auditor must advise Background Screening Credentialing Council (BSCC). BSCC must review specifics of case to determine whether organization may proceed with the accreditation process.
2.8 Agreement from Client			
Before providing subject reports to clients, organization must have and follow a procedure to obtain a signed agreement, certification, affirmation or other signed document from client in which client agrees to include all required contract provisions and that it will meet the requirements of all applicable law and regulation. If the jurisdiction uses the definitions of Controller and/or Processor (or similar terms) in the data protection regulations, the Agreement should specify which function each party belongs to.	Organization must provide written policy, procedure, or other written documentation describing when and how clients sign required agreement, certification, affirmation, or other document in which client agrees to comply with all applicable law and regulation and where such agreements are retained. organization must also provide copy of such agreement.	Organization must present written procedure for obtaining signed agreement, certification, affirmation, or other document, copy of signed agreement, and demonstrate where/how signed agreements are retained. Organization must make available the person responsible for retaining these agreements and auditor may ask to see (but not retain a copy of) signed agreements from one or more clients. Organization workers responsible for activating client access to organization systems/products must demonstrate knowledge that pre-requisites exist before client is permitted access to organization's products/ systems and how the organization worker knows it is permissible to activate access. If the jurisdiction uses the definitions of Controller and/or Processor (or similar terms) in the data protection regulations, the Agreement should specify which function each party belongs to. Organization must provide evidence of adherence to procedures.	Organization must provide documentation describing how signed agreements, certifications, affirmations, or other documents are obtained and retained. The agreement must meet requirements of any local requirements. Minimal information required in the Agreement includes: 1) permissible purpose, 2) requirement to provide notice and obtain authorization, where allowed, from the data subject, 3) an indication of who is in the roles of Controller / Processor, or equivalent, if this exists in the jurisdiction 4) confidentiality requirements, 5) compliance with all applicable laws and regulations, 6) that client will not use subject information in violation of law. Auditor will seek evidence of adherence to policies and procedures.
2.9 Client Legal Responsibilities			
Organization must have and follow procedures to inform client that client has legal responsibilities when procuring and using subject reports for background screening purposes. Organization must recommend to client that client work with legal counsel to ensure compliance with their specific legal responsibilities.	Organization must provide written agreements, policy, procedure, and related documentation describing how/when clients are informed that client has legal responsibilities when procuring and using subject reports for background screening purposes and when/how organization informs clients of necessity of consulting with their legal counsel regarding client's specific legal responsibilities.	Organization must present written procedure for informing client that client has legal responsibilities and advising client to consult with legal counsel. Organization must make available the document(s) used to so inform clients, the person responsible for retaining signed acknowledgments, and auditor may ask to see (but not retain a copy of) signed acknowledgments from one or more clients.	Organization must: 1) inform clients that client has legal responsibilities, and 2) advise client to consult with legal counsel. Methods include but are not limited to client agreement, user agreement, or some other document which is signed by the client and includes, but is not limited to, client acknowledgement of legal responsibilities. Current legal responsibilities include: 1) having permissible purpose, 2) disclosing to subject, 3) obtaining subject authorization, 4) following prescribed adverse action procedures, 5) complying with all applicable legal and regulatory requirements, and 6) obtaining, retaining, using, and destroying data in a confidential manner. Auditor will seek evidence of adherence to policies

		Organization must provide evidence of adherence to procedures.	and procedures.
2.9 a) Use Limitation			
Organization must have a process to notify controllers or clients except where prohibited by law, of the limitations on disclosure of Personal Data. Such reasons may include 1) with the consent of the subject or 2) by the authority of law (where judicial or other government subpoenas, warrants or orders require such disclosure).	Organization must notify controllers or clients of the limitations on use of Personal Data. Subjects must be informed as to why Personal Data is collected and the purpose(s) for which it will be used and maintained which includes 1) with the consent of the subject; or 2) by the authority of law.	Organization must demonstrate they have procedures in place for notifying controllers and clients of the limitations on disclosure of Personal Data to include 1) with the consent of the subject or 2) by the authority of law (where judicial or other government subpoenas, warrants or orders require such disclosure) and must provide the necessary training to organization workers regarding this subject. If interviewed, organization workers responsible for handling such disclosures, or responding to client requests for same, must demonstrate knowledge of the process and be able to access current documentation or refer the matter to whomever is responsible for such disclosures.	Organization must provide evidence of legal instruments (e.g., contracts), policy and procedures in place to ensure controller, clients and organization workers' understanding and agreement on limited use and disclosure of Personal Data. If such disclosure is not permissible, the agency must provide regulations which prohibit such disclosure and auditor will document the same.
2.10 Client Required Documents			
Organization must have and follow procedures to inform client of specific forms or documents required to complete specific searches.	Organization must provide written policy, procedure, or other documentation describing how/when clients are informed of specific forms or documents which are required for completion of a search the client has requested.	Organization must present written procedure describing how/when clients are informed of specific forms or documents that are necessary in order to complete one or more of the searches requested by the client. Organization must make available person responsible for informing clients of specific forms or documents required to complete specific searches, and auditor may ask to see (but not retain a copy of) completed forms or documents. Organization must provide evidence of adherence to procedures.	Organization must have and follow procedures to inform client of specific forms or documents required to complete specific searches. Auditor will seek evidence of adherence to policies and procedures.
2.11 Notice and Consent			
Organization must have and follow a procedure to inform client of legal requirements imposed by local regulations regarding notice or disclosure to and obtaining consent or authorization, if appropriate, from subjects prior to requesting a subject report from organization. Organization must recommend to client that client consult with counsel to develop a legally compliant notice and consent process.	Organization must provide written policy, procedure, or other documentation describing how/when clients are informed of legal requirements imposed by local regulations regarding providing disclosure to and obtaining authorization from subject prior to requesting a subject report from organization. Organization must also provide copy of document used to recommend to client that client consult with counsel to develop legally compliant disclosure and authorization policy and procedures.	Organization must present written procedure for informing client of legal requirements regarding notice and consent and advising client to consult with legal counsel. Organization must make available the document(s) used to so inform clients, the person responsible for retaining signed acknowledgments, and auditor may ask to see (but not retain a copy of) signed acknowledgments from one or more clients. If interviewed, organization workers must demonstrate knowledge of client's requirement to follow notice and consent processes, be able to access current copy of documentation; and/or workers must identify person(s) to address such topics. Organization must provide evidence of adherence to procedures.	Organization must inform client of legal requirements regarding notice and consent. Methods include, but are not limited to, inclusion in client agreement, user agreement or through some other document which is signed by the client and includes client acknowledgement. Auditor will seek evidence of adherence to policies and procedures.
2.13 Subject Disputes			

Organization must have and follow procedures for handling and documenting a subject dispute. At a minimum, procedures must meet all applicable legal and regulatory requirements and contain provisions around when such disputes should be referred to the client, if appropriate.	Organization must provide written policy, procedure, or other documentation which instructs organization workers on subject dispute procedures.	Organization workers responsible for subject disputes must demonstrate knowledge of proper subject dispute procedures, including when a dispute should be referred to the client, if appropriate, and be able to access current copy of documentation. Auditor may request to see a copy of dispute documentation and redacted examples of subject dispute processing. Organization must provide evidence of adherence to procedures.	The policies and procedures designed to handle subject disputes must meet local law requirements. In addition, organization must document: 1) responsibility of organization worker receiving subject dispute, 2) how incoming subject dispute letters/emails/phone calls must be routed upon receipt, 3) re-investigation responsibility and/or procedures, 4) process for updating/correcting subject report, 5) recordkeeping, 6) procedure to help prevent future occurrences (such as recommendation for training, software change, etc.), 7) consider information provided by subject, 8) advise subject if dispute is deemed frivolous or irrelevant, 9) notify appropriate parties of dispute results, and 10) comply with subject request for description of re-investigation process. Auditor will seek evidence of adherence to policies and procedures.
2.14 Database Records			
When reporting record information which is likely to have an adverse effect on a subject the organization shall maintain procedures designed to ensure the reported information is complete and is being reported accurately from the source.	Organization shall provide written policy, procedure, or other documentation describing method(s) used to comply with current organization requirements of maintaining procedures designed to ensure information is complete and up to date prior to reporting, or providing notice to the subject at the time information is reported to user of the subject report.	Organization workers responsible for reporting record information which is likely to have an adverse effect on a subject and shall demonstrate knowledge of procedures and be able to access current documentation.	The policy/procedure should maintain strict procedures designed to ensure the reported information is complete and is being reported accurately from the source.
2.15 Identification Confirmation			
Organization must have and follow procedures requiring reasonable procedures to assure maximum possible accuracy when determining the identity of a subject who is the subject of a record prior to reporting the information. In the case of name search only services, the organization shall use all reasonably available information to ensure the data being reported can be matched to the subject.	Organization must provide written policy, procedure, or other written documentation describing reasonable procedures used to assure maximum possible accuracy when determining the identity of a subject who is the subject of a record prior to reporting the information.	Organization must present written reasonable procedures to assure maximum possible accuracy when determining the identity of a subject who is the subject of a record prior to reporting the information. Organization shall make available the person responsible for ensuring compliance with organization's policy in regard to assuring maximum possible accuracy. Organization workers responsible for such identification must demonstrate knowledge of identification requirement and be able to access current documentation. Organization must provide evidence of adherence to procedures.	Reasonable procedures to assure maximum possible accuracy must include, but are not limited to: 1) matching a minimum of two identifiers where one identifier is first name + middle name/middle initial where available + last name (or reasonable derivative thereof); and second identifier is: a) month of birth + day of birth + year of birth, b) personal identification number, c) driver's license number, d) passport or country identification number, e) current or previous addresses, or f) multiple partial identifiers as defined in a) through e); OR 2) Any reasonable procedures that are demonstrably as effective as those described in 1. Auditor will seek evidence of adherence to policies and procedures. A clear name match only process must also be defined in cases where the search is based solely on subject name.
2.16 Subject Access Requests			
Organization must have and follow procedures for documenting and responding to subject access requests or refer them to client, if appropriate.	Organization must provide written policy, procedure, or other documentation which: 1) instructs organization workers on procedures to comply with subject request for all information in subject's file, and 2) describes how records of such requests and responses are created and maintained, 3) describes situations and procedures when such requests will be referred to a Controller (if legally allowed in the country).	Organization workers responsible for responding to subject request for subject access requests must demonstrate knowledge of proper procedures and be able to access current copy of documentation and outline process for when the request must be referred to the client. Organization must make available the person responsible for ensuring compliance with organization's policy in regard to providing all information in subject's file. Organization workers responsible for providing such information must demonstrate knowledge of requirement and be able to access current documentation. organization must provide evidence of adherence to procedures.	The policies and procedures designed to handle subject access requests must meet local law requirements, including the requirement for organization to obtain proper identification from the subject or refer the request to the client. Auditor will seek evidence of adherence to policies and procedures.

2.17 Jurisdictional Knowledge			
The organization must employ or have access to a qualified individual(s) within the organization or through a designated service provider, who is responsible for understanding search specifics, including terminology, as well as understanding the various jurisdictional and result differences.	Organization must employ or have access to a qualified individual(s) within the organization or through a designated service provider, who is responsible for understanding the details of background searches including search terminology, as well as understanding the various jurisdictional and search result differences. If multiple people are responsible, one person must hold overall responsibility as evidenced by written job description or other documentation.	Organization must present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for search knowledge. If a vendor is used to support this requirement, the vendor's evidence must be provided. Organization must make this person available in person, by phone, or organization shall provide signed affidavit. If interviewed, this individual shall demonstrate knowledge of search specifics as well as identifying resources for additional information. If interviewed, organization workers shall identify the person(s) who can provide search expertise when needed.	To be qualified, the individual must have one or more of the following: 1) criminal justice degree, 2) law enforcement experience, 3) legal experience, 4) court experience, 5) investigator experience, 6) a compliance and/or privacy qualification and/or 7) three years' work experience with court records and or background screening research. If a vendor is used to fulfill this requirement, evidence must be provided to support the vendor-organization relationship and confirmation that the vendor supports the organization with this knowledge requirement.
2.18 Automated Fulfillment			
If organization uses automated fulfillment systems, organization must have and follow reasonable procedures to ensure results as reported on subject report accurately reflect source information and to ensure that legal obligations around automated decision making are met, if applicable.	Organization must provide written policy, procedure, or other documentation defining methods used to monitor accuracy of automated reporting systems.	Organization must present procedures to monitor accuracy of automated system(s) results and take corrective actions when necessary. Organization shall make available to auditor tools or systems used. If interviewed, organization workers responsible for automated fulfillment systems must demonstrate knowledge of methods, must be able to access current copy of documentation, and must identify person(s) responsible for providing on-the-job leadership. Organization must provide evidence of adherence to procedures.	Procedures for auditing automated fulfillment systems must include, but are not limited to: 1) results as reported on subject report accurately reflect source information received into the automated system, 2) quantifying quality lapses, if any, 3) analyzing nature of lapses if any, 4) conducting root cause analysis, if any, and 5) developing and implementing appropriate corrective actions, if any. Procedures must include retention of monitoring records. Auditor will seek evidence of adherence to policies and procedures.
2.19 Quality			
Organization must have and follow procedures to reasonably ensure the accuracy and quality of all work product. Organization must have and follow accuracy and quality procedures specific to work product. The organization must take into account the particular nature of the search type and reporting when designing and implementing the specific procedures related to accuracy, completeness, and currency of the results, especially those likely to have an adverse effect on subjects. Organization must designate an individual(s) or position(s) within the organization responsible for quality.	Organization must provide written policy, procedure, or other documentation describing the procedures used to reasonably ensure the accuracy and quality of all work product, and procedures specific to work products likely to have an adverse effect on subject.	Organization must present procedures which are in place to reasonably ensure the accuracy and quality of all work-product, and procedures specific to work product. Organization shall make available to auditor tools or systems used (except actual personally identifiable information) to reasonably ensure accuracy and quality in all work product. If interviewed, organization workers responsible for work product must demonstrate knowledge of accuracy and quality requirements, describe methods used to ensure quality and accuracy, be able to access current copy of documentation, and identify person(s) responsible for providing on-the-job quality and accuracy leadership. Organization must provide evidence of adherence to procedures.	Organization must provide information regarding quality and accuracy of work product to organization workers who are responsible for such quality and accuracy by using various methods which include, but are not limited to: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or 5) availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual must be used. Auditor will seek evidence of adherence to policies and procedures.
	Organization must employ a minimum of one person who is responsible for organization's quality as evidenced by written job description(s) or other	Organization must present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible	Organization quality leader must affirm his/her role as being responsible for quality within the organization and be able to demonstrate sufficient authority to effectively fulfill their role.

	documentation. If multiple people are responsible, one person must hold overall responsibility as evidenced by written job description or other documentation	for quality. Organization must make this person available either in person or by phone. If interviewed, organization workers must identify the person(s) responsible for quality.	

2.20 Reappearance of Inaccurate Information			
Organization must have and follow procedures to prevent reappearance of inaccurate subject information in subject reports, as permitted by law and client contracts.	Organization must provide written policy, procedure, or other written documentation describing procedures used to prevent reappearance of inaccurate subject information in subject reports.	Organization must present written documentation for preventing reappearance of inaccurate subject information in subject reports. Organization must make available the person responsible for ensuring compliance with organization's policy in regard to preventing reappearance of inaccurate subject information. Organization workers responsible for such prevention must demonstrate knowledge of prevention requirement and be able to access current documentation. Organization must provide evidence of adherence to procedures.	Procedures must include process by which re-reporting of inaccurate information is prevented. Procedures must include, but are not limited to: 1) identifying subjects who previously had inaccurate information reported, who disputed such information, and for whom organization removed or otherwise corrected inaccurate information, 2) method(s) by which previously reported inaccurate information is prevented from being included in new reports, and 3) process/method by which previously received inaccurate information is corrected and recorded in automated reporting systems, where applicable. Auditor will seek evidence of adherence to policies and procedures.
2.21 Quality Analysis			
Organization must have and follow procedures to audit and analyze product quality. Identified quality lapses, including those identified during subject disputes, must be quantified and analyzed, including root cause analysis, and appropriate corrective actions must be implemented.	Organization must provide written policy, procedure, or other documentation describing the methods used to quantify and analyze quality failures, including root cause analysis, and implement appropriate corrective actions. Procedures must include two types of quality testing: 1) work product initially free of defect, and 2) work product containing quality failures (whether identified internally or through subject dispute).	Organization must present written documentation to quantify and analyze quality lapses, including root cause analysis, and implement appropriate corrective actions. Organization shall make available to auditor tools or systems used (except actual personally identifiable information). If interviewed, organization workers responsible for quality analysis must demonstrate knowledge of methods, must be able to access current copy of documentation, and must identify person(s) responsible for providing on-the-job quality analysis leadership. Organization must provide evidence of adherence to procedures.	Procedures for quality control and analysis must include, but are not limited to: 1) an established protocol for systematically sampling results provided in subject report, 2) quantifying quality lapses, 3) analyzing nature of lapses, 4) process for conducting root cause analysis, and 5) developing and implementing appropriate corrective actions. Procedures must include retention of monitoring records. Auditor will seek evidence of adherence to policies and procedures.
Client Education			
3.1 Truth in Advertising			
Organization must have and follow a procedure to communicate to clients the original source type (records, data files, employer, academic institution, etc.), limitations, variables affecting the information available and scope of information provided by each screening product offered by the organization.	Organization must provide written policy, procedure, or other documentation describing how/when clients are provided with information that describes the composition of each product, type of information source(s) used for each product, factors affecting the information, and any parameters or conditions applied by the organization when reporting to client. Organization must provide copy of documents used to so inform clients. If organization provides actual subject reports to demonstrate full and accurate product	Organization must present written procedure for providing information to clients that accurately describes products, including one or more samples of provided documents. If subject reports are used to demonstrate full and product disclosure, all personally identifiable information must be redacted and auditor will not retain copy. If interviewed, organization workers must demonstrate knowledge that product descriptions exist, where such descriptions are retained, and/or the person responsible for	Organization must inform clients of specific composition of background screening products. Information disclosed regarding products must include, but is not limited to: 1) type of source, 2) scope of records searched, and 3) search methodology. It is recommended that disclosure of information source, type of source, scope of search, and search methodology be included in subject reports. Lacking such disclosure, reports should explain how user of the report may obtain such information. Auditor will seek evidence of adherence to policies and procedures.

	disclosure, all personally identifiable information must be redacted.	organization's products. Organization must provide evidence of adherence to procedures.	
3.2 Legal Counsel			
Organization must have and follow a procedure to inform client that organization is not acting as legal counsel and cannot provide legal advice. Organization must inform client of the importance of working with counsel to develop a background screening program specific to their needs and to ensure that client's policies and procedures related to the use of organization-provided information are in compliance with all applicable legal and regulatory requirements.	Organization must provide written policy, procedure, or other documentation describing how/when clients are informed that organization is not acting as legal counsel and cannot provide legal advice. Organization must provide copy of document used to so inform client and such document must include advising client to work with legal counsel regarding client's specific screening program, policies, and procedures to ensure legal compliance.	Organization must present written procedure for informing client that organization does not provide legal advice or act as client's legal counsel. Organization must make available the document(s) used to so inform clients, the person responsible for retaining signed acknowledgments, and auditor may ask to see (but not retain a copy of) signed acknowledgments from one or more clients. If interviewed, organization workers must demonstrate knowledge of organization's position that legal counsel is not provided, be able to access current copy of documentation, and/or organization workers must identify person(s) to address legal topics. organization must provide evidence of adherence to procedures.	Organization must inform clients that organization does not function as legal counsel. Methods include, but are not limited to, inclusion in client agreement, user agreement or through some other document which is signed by the client and includes client acknowledgement. Such acknowledgment must include, but is not limited to: 1) organization is not legal counsel and does not provide legal advice, 2) advising client of importance of working with their legal counsel to ensure overall screening program compliance, and 3) advising clients that subject reports provided by organization must be used in compliance with all applicable legal and regulatory requirements. Auditor will seek evidence of adherence to policies and procedures.
3.3 Understanding Subject Reports			
Organization must have and follow a procedure to provide guidance to client on how to order, retrieve, read and understand the information provided in subject reports provided by the organization.	Organization must provide written policy, procedure, or other documentation describing how/when clients are provided with information regarding obtaining and understanding subject reports. Organization must provide copy of document(s) used to so inform client, must demonstrate online tools/information (such as User Guide or online Help) provided to clients, or other method(s) used to assist clients.	Organization must present written procedure for informing client how to obtain and understand subject reports from organization. Organization must make available the documents or systems used to so inform clients. If interviewed, organization workers must demonstrate knowledge of how such education is provided, be able to access current copy of documentation, and/or organization workers shall identify person(s) to address such topics. Organization must provide evidence of adherence to procedures.	Organization must provide information to clients regarding how to order, retrieve, read, and understand subject reports by using 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. Auditor will seek evidence of adherence to policies and procedures.
3.4 Information Protection			
Organization must have and follow a procedure to inform client of: 1) the sensitive nature of subject reports, 2) the requirement to protect such information, and 3) the subject report retention and destruction practices as outlined in the Fair Information Privacy Principles (FIPPs).	Organization must provide written policy, procedure, or other documentation describing how/when clients are informed regarding the importance of and legal requirement to protect subject data presented in subject reports. Organization must provide copy of document(s) used to so inform client.	Organization must present written procedure for informing client of client's legal responsibilities regarding protection of subject data. Organization must present the document(s) used to so inform clients, the person responsible for retaining signed acknowledgments, and auditor may ask to see (but not retain a copy of) signed acknowledgments from one or more clients. If interviewed, organization	Organization must inform clients of client's legal requirements regarding protection of subject data. Methods include, but are not limited to, inclusion in client agreement, user agreement or through some other document which is signed by the client and includes, but is not limited to, client acknowledgement of subject data protection responsibilities. Per the FIPPs, current requirements include: 1) limiting dissemination of subject information to only those with legitimate need, permissible purpose, and authorized by subject, 2) retaining subject data in a confidential manner, and 3) destroying data in a secure manner.

		workers must demonstrate knowledge of client's requirement to protect subject data, be able to access current copy of documentation; and/or organization workers shall identify person(s) to address such topics. Organization must provide evidence of adherence to procedures.	
Researcher and Data Standards – Third Party Service Providers			
4.1 Third Party Service Provider (Vendor/Agent) Agreement			
Organization must have and follow a procedure requiring a signed agreement, which may include amendments and/or addenda, from all third party service providers who have access to a subject's personal information and who handle that information on the organization's behalf or direction. The agreement must clearly define the scope of services to be provided, confidentiality requirements, and other obligations as outlined by law or client contract.	Organization must provide written policy, procedure, or other written documentation describing how a signed agreement covering scope of services is obtained from and retained for all vendors and agents. Organization must also provide copy of current agreement. (Note: This agreement may also incorporate Certification requirements of Clause 4.3.)	Organization must present written procedure for obtaining signed agreement, copy of agreement, and demonstrate where/how signed agreements are retained. Organization must make available the person responsible for obtaining and retaining these agreements and auditor may ask to see (but not retain a copy of) signed agreements from one or more vendors and agents. If interviewed, organization workers responsible for working with vendors and agents must demonstrate understanding of requirement for signed agreement prior to utilizing services of vendors and agents OR technology must prevent utilization of vendor or agent by organization workers until organization leader has enabled use. organization must provide evidence of adherence to procedures.	The agreement may include, but is not limited to: 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 including secure transmission of information and proper retention and disposal practices, 9) other obligations under law, and 10) requirement for vendor or agent to obtain a similar agreement from subcontractors, if subcontractors or sub-processors are used. Auditor will seek evidence of adherence to policies and procedures. Do the mechanisms referred to above generally require that sub-processors: a) Follow-instructions provided by the organization relating to the manner in which personal information must be handled? b) Impose restrictions on further sub-processing c) intentionally removed d) Provide the organization with self-assessments or other evidence of compliance with instructions and/or agreements/contracts? If YES, describe. e) Allow the organization to carry out regular spot checking or other monitoring activities? If YES, describe.
4.2 Vetting Requirement			
Organization must have and follow procedures to vet new third party service providers. Procedures must include criteria for ensuring service providers can enable both compliance with applicable law as well as these Clauses. Due diligence procedures must be undertaken prior to the engagement of any service provider who processes Personal Data.	Organization must provide written policy, procedure, or other written documentation describing the requirement to and methodology used to vet new vendors or agents.	Organization must present written procedure for vetting new third party service providers, and demonstrate where/how records are retained. Organization shall make available the person responsible for such vetting and auditor may ask to see (but not retain a copy of) vetting records from one or more. If interviewed, organization workers responsible for working with providers must demonstrate understanding of vetting requirement prior to utilizing services of third party service provider OR technology must prevent utilization of third party service provider by organization workers until organization leader has enabled use. Organization	The vetting records must include, but are not limited to: 1) evidence of right to conduct business as is available. (This may be a copy of business license, articles of incorporation, or at the least an explanation of what is required in that jurisdiction to run such a business and proof of meeting this. In some jurisdictions, organizations must be registered. Proof of registration is requested, and preferably obtained as a third party), 2) completed favorable reference interview from at least one current client, and 3) verification of association memberships, which should be verified with the association where possible. Auditor will seek evidence of adherence to policies and procedures.

		must provide evidence of adherence to procedures.	
Organization must present proof of errors and omissions insurance coverage, equivalent business insurance coverage, or self-insurance of $1 million (or equivalent in local currency) if such coverage is commonly available or required in countries of operation. If such insurance coverage is not commonly available, organization shall provide attestation of same and of organization's financial ability to withstand claims based on its operation and clause in client agreement may outline how issues will be resolved should they arise.	Organization must provide copy of Certificate of Insurance listing errors and omissions policy coverage amount. If organization does not maintain errors and omissions insurance because it is not common practice or not available in their country of operation, organization must provide documentation or self-attestation that they have self- insured, are aware of the potential financial risks related to their operation, or can otherwise demonstrate the financial ability to pay should an issue arise.	None	None
4.5 Information Security			
Organization must have and follow a procedure providing a secure means by which third party service providers will receive orders and return search results.	Organization must provide written policy, procedure, or other written documentation describing the requirement to and method used to secure and protect subject information when such information is being transmitted to and returned by vendors or agents.	Organization must present written procedure for sending subject information to and receiving subject information from and obtain signed agreement from the third party service provider to that effect. Organization must make available the person responsible for security of transmitted subject information. For each transmission method, organization may be asked to demonstrate, or provide written documentation of, the security controls which are in use. Organization must provide evidence of adherence to procedures.	Security procedures, which must be agreed to in writing by the third party service provider, for transmission of personally identifiable information to/from, must include, but are not limited to use of an electronic system designed for secure transmission of information between organization and third party service provider; or if other transmission methods are used, security procedures must include, but are not limited to: 1) all transmissions must directed to a named party, 2) all transmissions must be clearly marked as "CONFIDENTIAL" and include a request to notify sender if received by someone other than named party, 3) if faxed, a cover page must always be used and must not contain any personally identifiable information, 4) if faxed, organization must have verified receiving fax is in a non-public location, 5) if transmitted via the Internet, data must be securely encrypted using a currently recognized standard. Auditor will seek evidence of adherence to policies and procedures.
4.6 Auditing Procedures			
Organization must have and follow a procedure to monitor the quality and accuracy of active third party service providers.	Organization must provide written policy, procedure, or other written documentation describing the requirement to and method used to monitor the quality and accuracy of vendors or researchers.	Organization must present written documentation for monitoring. Organization shall make available the person responsible for such audits and auditor may ask to see (but not retain copy of) documentation of such monitoring. Organization must provide evidence of adherence to procedures.	Monitoring procedures for must include, but are not limited to: 1) an established protocol for auditing, 2) volume of audit to be conducted, 3) sending research requests where result is already known (where allowable by law or source), 4) how returned results are compared to expected results, and 5) process for dealing with errors up to and including termination of services. Test cases, where allowed by law or source, must be entered in a log with results including: A) date of test, B) unique identifier, C) results returned, D) whether results were as expected, and E) any remedial actions taken. Auditor will seek evidence of adherence to policies and procedures.
Verification Services Standards			
5.1 Verification Accuracy			
Organization must have and follow reasonable procedures to assure maximum possible accuracy when obtaining, documenting and reporting search information.	Organization must provide written policy, procedure, or other documentation used to reasonably ensure accuracy and thoroughness in the search process.	Organization must make available to auditor tools or systems used (except actual personally identifiable information) to reasonably ensure search result	Organization must provide information regarding search accuracy to workers who are responsible for such accuracy by using various methods which may include, but are not limited to: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job

		accuracy. If interviewed, organization workers responsible for search accuracy must demonstrate knowledge of accuracy requirement; describe methodology by which they learn how to obtain and report accurate results. Organization workers responsible for search accuracy shall be able to access current copy of documentation; AND/OR organization workers must identify person(s) responsible for accuracy. organization must provide evidence of adherence to procedures, including training records.	training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual must be used. In cases other than name match only services, methods used to reasonably ensure search accuracy must include, but are not limited to: the use of a minimum of two identifiers for all result reporting, 1) confirmation of identity through verification of unique personal identifier, full name, and/or date of birth; and 2) confirmation of information source name, address, and contact information. Auditor will seek evidence of adherence to policies and procedures, which may include training records.
5.2 Current Employment			
Organization must have and follow procedures to contact subject's current employer directly only when authorized by subject or when client receives authorization from subject and provides such authorization to organization.	Organization must provide written policy, procedure, or other documentation used to ensure subject's current employer is not contacted directly unless subject has provided explicit authorization or when client receives authorization from subject and provides such authorization to organization.	Organization must make available to auditor tools or systems used (except actual personally identifiable information) to reasonably ensure current employer is not directly contacted without explicit authorization by the subject or the client on behalf of the subject. If interviewed, organization workers responsible for verification of current employment must demonstrate knowledge of authorization requirement and describe methodology by which they learn about such requirement. Organization workers responsible for current employer contact must be able to access current copy of documentation; and/or organization workers must identify person(s) responsible for such contact. organization must provide evidence of adherence to procedures, including training records.	Organization must provide information regarding verification of current employment to organization workers who are responsible for such verification by using various methods which must include, but are not limited to, at least one of the following: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual may be used. Methods used to reasonably ensure subject's current employer is directly contacted only with authorization may include, but are not limited to: 1) authorization provided on employment application, 2) explicit authorization provided within Disclosure/ Authorization signed by subject, 3) specific directive provided by client following receipt of authorization from subject, and/or 4) technology must prevent verification of current employment by organization workers until organization Leader has so enabled. Auditor will seek evidence of adherence to policies and procedures, which may include training records.
5.3 Accredited or Authenticated Academic Institutions			
Organization must have and follow procedures to inform client what steps have been taken to authenticate the institution itself. The procedures must also include steps to verify the accuracy of the information provided against the details provided by the subject and to flag any concerns which may exist with the information obtained or the institution from which it was obtained. If an institution is suspected of being a diploma mill or otherwise suspect in their operations, clients should be directed to verify the legitimacy of same.	Organization must provide written policy, procedure, or other documentation used to determine whether post-secondary academic institution has been reviewed for authenticity. The procedures must also include steps to verify the accuracy of the information provided against the details provided by the subject and to flag any concerns which may exist with the information obtained or the institution from which it was obtained. If an institution is suspected of being a diploma mill or otherwise suspect in their operations, clients should be directed to verify the legitimacy of same.	Organization must provide policy or procedure used to reasonably ensure accreditation status of post-secondary academic institution and to inform client when any academic institution submitted for verification is not accredited by an accrediting body recognized by the country. The procedures must also include steps to verify the accuracy of the information provided against the details provided by the subject and to flag any concerns which may exist with the information obtained or the institution from which it was obtained. If an institution is suspected of being a diploma mill or otherwise suspect in their operations,	Organization must provide information regarding verification of accreditation status of post-secondary academic institutions to organization workers who are responsible for such verification by using various methods which include, but are not limited to, at least one of the following: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual must be used. Methods used to reasonably ensure legitimacy of accrediting body include, but are not limited to confirmation using: comparable global body, if reasonably available. Auditor will seek evidence of adherence to policies and procedures, which may include training records.

		clients should be directed to verify the legitimacy of same. If interviewed, organization workers responsible for verification of academic credentials must demonstrate knowledge of accrediting bodies and describe methodology by which they learn how to confirm accreditation status of academic institutions.	
Recognizing that degree requirements are not globally equivalent, and that sometimes similarly named degrees are very different, Organization must have and follow procedures to recommend to client that when specific degree requirements are critical to the job to be filled, that the client consider degree equivalency evaluation as an additional service.	Organization must present written policy, procedure, client education material or other written documentation used to recommend to client that when specific degree requirements are critical to the job to be filled, that the client consider degree equivalency evaluation as an additional service.	Recognizing that degree requirements are not globally equivalent, and that sometimes similarly named degrees are very different, Organization must have and follow procedures to recommend to client that when specific degree requirements are critical to the job to be filled, that the client consider degree equivalency evaluation as an additional service. Organization workers responsible for verification of academic credentials must be able to access current copy of documentation; AND/OR organization workers must identify person(s) responsible for such activity. Organization must provide evidence of adherence to procedures, including training records.	Organization must provide documentation used to recommend to client that when specific degree requirements are critical to the job to be filled, that the client consider degree equivalency evaluation as an additional service.
5.4 Procedural Disclosures			
Organization must have and follow procedures to provide full disclosure to clients about general business practices regarding number of attempts to verify information, what constitutes an "attempt," locate fees, fees charged by the employer or service provider and standard question formats prior to providing such services.	Organization must present written policy, procedure, client education material or other written documentation used to provide full disclosure to a client about general business practices regarding number of attempts to verify information, what constitutes an "attempt," locate fees, fees charged by the employer or service provider and standard question formats prior to providing such services.	Organization must make available to auditor tools or systems used to disclose to client general practices regarding verification practices including attempts to verify, fees, question formats, etc. organization must present written procedure for providing information to clients that accurately describes products, including one or more samples of provided documents. If subject reports are used to demonstrate full and accurate procedural disclosure, all personally identified information must be redacted and auditor will not retain copy. If interviewed, organization workers must demonstrate knowledge that procedural requirements exist, where such requirements are documented, and/or the person responsible for organization's products. Organization must provide evidence of adherence to procedures.	Organization must provide information to clients regarding general verification business practices by using various methods which may include, but are not limited to: 1) product descriptions, 2) statement of work documents, 3) written agreements, and/or detail provided in the verification itself. Disclosed information regarding general verification business practices must include, but is not limited to: 1) number of attempts to verify information, 2) what constitutes an "attempt," 3) fees charged by the employer or service provider, and 4) standard question formats. Auditor will seek evidence of adherence to policies and procedures.
5.5 Verification Databases			
If organization compiles, maintains and resells employment or educational verification information, organization must have and follow procedures to ensure that data compiled and stored is accurate, including procedures for handling subject disputes and subject access requests. If databanking of subject	Organization must present written policy, procedure or other written documentation used to ensure that data compiled and stored is accurate, including procedures for handling subject disputes. If organization does not compile, maintain, and resell employment or education	Organization must make available to auditor tools or systems used (except actual personally identifiable information) to reasonably ensure data compiled and stored is accurate. If interviewed, organization workers responsible for accuracy of stored data must	This clause addresses organizations that compile information for potential future use or sale. Organization must provide information regarding accuracy of stored data to organization workers who are responsible for such accuracy by using various methods which include, but are not limited to, at least one of the following: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide

information is not permissible in the country(ies) of service, the organization shall provide a statement to that effect in their procedures.	information, or such retention is not permissible in their jurisdiction(s), the organization must provide written affirmation to that effect.	demonstrate knowledge of accuracy requirement and describe methodology used to ensure accuracy. Organization workers responsible for accuracy of stored data must be able to access current copy of documentation, identify person(s) responsible for accuracy of stored data, AND/OR utilize technology to control the addition or deletion of information in the database(s). Organization must provide evidence of adherence to procedures, including training records.	assistance when needed. If classroom or on-the-job training is used, a training outline or manual must be used. Methods used to reasonably ensure accuracy of stored data include, but are not limited to: criteria for inclusion into the database, criteria for redaction from the database, criteria for correcting inaccuracies and handling subject disputes. This documentation must also outline how to respond to subject requests for access to their information. Auditor will seek evidence of adherence to policies and procedures, which may include training records.
5.6 Use of Stored Data			
If local jurisdictions allow and the organization provides results based in part or in total from previously reported data, the organization must have and follow procedures to ensure the reported information is current and up to date.	Organization must present written policy, procedure or other written documentation to ensure organization has and follows procedures to report only accurate and up to date information from previously used reports.	Organization must make available to auditor tools or systems used (except actual personally identifiable information) to reasonably ensure that previously reported information is current and up to date at the time of the repeat report. If interviewed, organization workers responsible for use of such data shall demonstrate knowledge of the process for verifying accuracy. Organization workers responsible for use of stored data must be able to access current copy of documentation; must identify person(s) responsible for use of stored data. If local jurisdictions allow and the organization provides results based in part or in total from previously reported data, the organization must have and follow procedures to ensure the reported information is current and up to date. Organization must provide evidence of adherence to procedures, including training records.	Organization must provide information regarding reuse of stored data to organization workers who are responsible for using such data by using various methods which include, but are not limited to, at least one of the following: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or 5) availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual must be used. Such information and/or training shall include what constitutes reuse of information and confirming accuracy and currency for different types of background checks through: 1) definition, 2) examples, and/or 3) by referring organization workers to designated expert. Auditor will seek evidence of adherence to policies and procedures, which may include training records.
5.7 Documentation of Verification Attempts			
Organization must have and follow procedures to document all verification attempts made and the result of each attempt, in completing all verification services.	Organization must present written policy, procedure, or other written documentation used to ensure that all attempts made to verify information are fully documented.	Organization must make available to auditor tools, systems, or methods used to capture attempts to verify and related information. If a manual process, organization must present written procedure for capturing such information. If subject reports are used to demonstrate captured attempts and related information, all personally identified information shall be redacted and auditor will not retain copy. If interviewed, organization workers must demonstrate knowledge that attempts to verify must be documented, where such requirements are documented, identify the person responsible for	Organization must provide information regarding attempts to verify and related information to organization workers who are responsible for data verification by using various methods which include, but are not limited to, at least one of the following: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual must be used. Information regarding attempts to verify must include, but is not limited to: 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 attempt, and 5) the organization worker who made the attempt or obtained information. Auditor will seek evidence of adherence to policies and procedures, which may include training records.

		organization's products and processes, AND/OR technology must automatically capture attempts to verify and related information. Organization must provide evidence of adherence to procedures, including training records.	
5.8 Outsourced Verification Services			
Organization must have and follow procedures requiring a signed agreement from all providers of outsourced verification services. The agreement must clearly outline the scope of services to be provided, verification methodology, documentation of verification efforts, disclosure of findings, time frame for communication and completion of requests, confidentiality requirements, and reinvestigation requirements to ensure the accuracy of information.	Organization must provide written policy, procedure, or other written documentation describing how a signed agreement covering scope of services is obtained from and retained for all current outsourced verification service providers. organization must also provide copy of current agreement. If organization does not outsource verification services, organization must provide written affirmation to that effect.	Organization must present written procedure for obtaining signed agreement, copy of agreement, and demonstrate where/how signed agreements are retained. Organization must make available the person responsible for obtaining and retaining these agreements and auditor may ask to see (but not retain a copy of) signed agreements from one or more outsourced verification service providers. If interviewed, organization workers responsible for working with these providers must demonstrate understanding of requirement for signed agreement prior to utilizing services of provider OR technology must prevent utilization of provider by organization workers until organization Leader has enabled use. Organization must provide evidence of adherence to procedures.	The agreement must include, but is not limited to: 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 organization workers, and 10) signed non-disclosure agreements from provider's organization workers. In particular, the agreement must emphasize confidentiality requirements including: A) the legal requirement to treat all subject information as confidential, B) secure data transmission, and C) secure and timely disposal of confidential information. Auditor will seek evidence of adherence to policies and procedures.
5.9 Conflicting Data			
Should organization receive information from the verification source subsequent to the delivery of the subject report, and as a direct result of the initial inquiry, that conflicts with originally reported information, and that new information is received after the initial report , (or as may be required by law). Organization must have and follow procedures to notify client of such information.	Organization must provide written policy, procedure, or other documentation describing how conflicting data, when received within 120 days of report completion and as a direct result of original inquiry, is provided to client who originally ordered such report.	Organization workers responsible for reporting conflicting data must demonstrate knowledge of proper procedures and be able to access current copy of documentation. Organization must provide evidence of adherence to procedures, including training records.	Organization must provide information regarding processing and reporting of conflicting data to organization workers who have this responsibility by using various methods which include, but are not limited to, at least one of the following: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual must be used. Information regarding handling and reporting of conflicting data must include, but is not limited to: 1) confirmation that conflicting information is specifically related to same subject, same client, and original report, 2) verification of the authenticity of the conflicting information and its source, 3) method used to update report, and 4) method used to provide updated information to subject and client, and 5) the form in which the update is provided. Auditor will seek evidence of adherence to policies and procedures, which may include training records.
5.10 Authorized Recipient			
If organization is requesting verification by phone, fax, email or	Organization must provide written policy, procedure, or	Organization must present written procedure for	Procedures used to ensure verification requests are sent to an authorized recipient must

mail, organization must have and follow procedures to confirm that verification request is directed to an authorized recipient.	other documentation used to require that verification requests are directed to authorized recipients.	confirming a verification request is being sent to an authorized individual. If interviewed, organization workers responsible for processing verification requests must demonstrate knowledge of proper authentication procedures and must be able to access current copy of documentation. Organization must provide evidence of adherence to procedures, including training records.	include, but are not limited to: 1) confirming method used by information source to provide verification information, 2) confirming company/institution name and address matches that provided by subject, and 3) obtaining name and title of person to whom request will be sent. Auditor will seek evidence of adherence to policies and procedures, which may include training records.

Business Practices			
6.1 Background Checks for Organization Personnel Charged with Enforcement of Policy			
Organization must have and follow a policy requiring criminal background checks and/or government sponsored sanction list checks be conducted on all organization owners, officers, principals and organization workers charged with enforcement of company policy, where allowed by law. Sanctions 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, or as allowed by local law. 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. Additional searches may also be conducted as required by law and / or client contract.	Organization must provide written policy, procedure, or other written documentation describing the requirement for and methodology used to conduct and retain criminal record and/or sanctions list checks on owners, principals, and organization workers charged with enforcement of company policy. The documentation must describe how results of these checks are evaluated in relation to any potentially negative results found and the individual's enforcement role. The documentation must include special processes used to evaluate convictions for any crimes involving dishonesty, fraud, moral turpitude, or listing on a government sponsored sanction list. If criminal records or sanctions checks are not allowed by local law, the organization should provide evidence of this restriction. If criminal and sanctions checks are not allowed, organization should provide evidence of their vetting program on this level of staff.	Organization must present written procedure for conducting criminal record and/or sanctions list checks (sanctions checks conducted at least once every two years) on owners, principals and organization workers charged with the enforcement of company policy. organization must demonstrate how results are reviewed, including the review of any results with potential derogatory information and where records are retained. Organization must make available the person responsible for these checks and auditor may ask to see (but not retain a copy of) check results. If sharing of organization worker data is not permissible in the jurisdiction where the organization operates, the designated compliance contact shall provide attestation of same. Organization must provide evidence of adherence to procedures. If criminal records or sanctions checks are not allowed by local law, the organization should provide evidence of this restriction and should provide evidence of their vetting program on this level of staff.	This clause refers only to the entity being accredited and not any parent company. It covers owners, managers, and organization workers charged with enforcement of company policy. If conviction(s) or sanctions listing(s) are found, the evaluation of such information must comply with all applicable legal and regulatory requirements in relation to work performed by organization and licenses held by the organization (such as private investigator), as well as a review of the process for evaluating any potential negative information Auditor will seek evidence of adherence to policies and procedures.
6.2 Background Checks for Organization Workers			
Organization must have and follow a policy requiring allowable criminal background checks and/or government sponsored sanction list checks be conducted on all organization workers. Sanctions checks must be conducted at least once every two years, where allowed by law, and records retained as long as organization worker provides services to organization, or as allowed by local law. Any criminal conviction(s) or sanctions listing(s) must be evaluated to determine if the individual may remain his/her current position or any other position with organization 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 or desired role. Additional searches may also be conducted as required by law and / or client contact. If criminal background and sanction checks are not permissible in the jurisdiction where the organization operates, the designated compliance contact shall provide attestation of same.	Organization must provide written policy, procedure, or other written documentation describing the requirement for and methodology used to conduct and retain criminal record and sanctions list checks on organization workers. The documentation must describe how results of these checks are evaluated in relation to any potentially negative results found and the individual's role. If criminal records or sanctions checks are not allowed by local law, the organization should provide evidence of this restriction. If criminal and sanctions checks are not allowed, organization should provide evidence of their vetting program on this level of staff.	Organization must present written procedure for conducting criminal record and/or sanctions list checks (sanctions checks conducted at least once every two years) on organization workers. If criminal background and sanction checks are not permissible in the jurisdiction where the organization operates, the designated compliance contact shall provide attestation of same and explain their vetting process for organization workers. Organization must demonstrate how results are reviewed, including the review of any results with potential derogatory information and where records are retained. Organization must make available the person responsible for these checks and auditor may ask to see (but not retain a copy of) criminal history and sanctions list check results. Organization must provide evidence of adherence to procedures.	If conviction(s) or sanctions listing(s) are found, the evaluation of such information must comply with all applicable legal and regulatory requirements in relation to work performed by organization and licenses held by the organization (such as private investigator), as well as a review of the process for evaluating any potential negative information. Auditor will seek evidence of adherence to policies and procedures.
6.3 Changing Law and Regulation			

Organization must have and follow procedures to remain knowledgeable about and compliant with changing law and regulation. The organization must designate an individual(s) or position(s) with the organization responsible for such knowledge and compliance or identify the external resource utilized for this purpose.	Organization must employ or retain a minimum of one person who is responsible for organization's knowledge of and compliance with changing law and regulation as evidenced by written job description(s) or other documentation. If multiple people are responsible, one person must hold organization Leadership role and overall responsibility as evidenced by written job description or other documentation.	Organization must present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for organization's knowledge of and compliance with changing law and regulation or external resource retained for such purpose. Organization must make this person available either in person or by phone. If interviewed, organization workers must identify the person(s) that can provide expertise in regard to changing law and regulation.	Responsible individual must affirm his/her role as being responsible for knowledge of changing law and regulation and compliance with same.
6.4 Insurance			
Organization must present proof of errors and omissions insurance coverage, equivalent business insurance coverage, or self-insurance of $1 million (or equivalent in local currency) if such coverage is commonly available or required in countries of operation. If such insurance coverage is not commonly available, organization shall provide attestation of same and of organization's financial ability to withstand claims based on its operation and clauses in client agreement may outline how issues will be resolved should they arise.	Organization must provide copy of Certificate of Insurance listing errors and omissions policy coverage amount. If organization does not maintain errors and omissions insurance because it is not common practice or not available in their country of operation, organization must provide documentation or self-attestation that they have self- insured, are aware of the potential financial risks related to their operation, or other can otherwise demonstrate a financial ability to pay should an issue arise.	None	None
6.5 Client Authentication			
Organization must have and follow a procedure to identify and authenticate all clients prior to disclosing subject reports or other subject information. The procedure must require the organization to maintain written records regarding the qualification of each client who receives subject reports or other subject information.	Organization must provide written policy, procedure, or other written documentation describing the requirement for and method used to authenticate clients prior to providing subject reports or any subject information to client. Organization must provide written policy, procedure, or other written documentation describing the requirement for and method used to determine authorization of clients to access specific Personal Data prior to providing subject reports or any subject information to client.	Organization must present written procedure for authenticating new clients, and demonstrate where/how authentication results are retained. Organization must make available the person responsible for such authentication and auditor may ask to see (but not retain a copy of) authentication records from one or more client companies. If interviewed, organization workers responsible for providing subject information to clients must demonstrate understanding of authentication requirement prior to providing subject information to clients or technology must prevent providing such information to clients until organization Leader has enabled process. organization must provide evidence of adherence to procedures.	Client authentication methods must include, but are not limited to: 1) obtaining evidence of right to conduct business, such as copy of business license, articles of incorporation, or government filing etc., and authentication thereof, 2) verification of working business phone, fax, email, and website, 3) verification of listing in business directories and may include 4) onsite inspection to confirm business facility exterior and interior appearance meet common business norms for this type of business. Auditor will seek evidence of adherence to policies and procedures.
6.6 Vendor Authentication			
Organization must have and follow a procedure to identify and	Organization must provide written policy, procedure, or	Organization must present written procedure for	In the case of vendors that are recognized and commonly utilized by organizations, a signed

authenticate all vendors prior to disclosing subject information. The procedure must require the organization to maintain written records regarding the qualification of each vendor who receives subject information.	other written documentation describing the requirement for and method used to authenticate vendors prior to disclosing any subject information to vendor.	authenticating new vendors, and demonstrate where/how authentication results are retained. Organization must make available the person responsible for such authentication and, if interviewed, this person must demonstrate understanding of authentication requirements. Auditor may ask to see (but not retain a copy of) authentication records from one or more vendor companies. organization must provide evidence of adherence to procedures.	agreement between the vendor and organization will suffice as authentication. Such vendors include: major 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, the following: 1) evidence of right to conduct business, such as copy of business license, articles of incorporation, or government filing etc., and authentication thereof, 2) verification of working phone/fax numbers, website, email, 3) reference through a minimum of one independent third party, and 4) previous experience of organization when working with vendor. Authentication records may also include onsite inspection results. Auditor will seek evidence of adherence to policies and procedures.
6.7 Subject Authentication			
Organization must have and follow reasonable procedures to obtain proof of identity prior to providing any information to a subject making a telephonic inquiry. The organization must maintain reasonable procedures to document the information used to identify each subject to whom subject information is provided.	Organization must provide written policy, procedure, or other written documentation describing how/when subject authentication/ identification occurs prior to disclosing subject information and where record of such authentication is kept.	Organization must present written procedure for confirming subject identity prior to providing any subject information to such person. Auditor may ask to see demonstration of subject identification, how organization representative confirms identity of subject, and where record of authentication is retained. Organization must provide evidence of adherence to procedures. If interviewed, organization workers responsible for handling such requests must demonstrate knowledge of and be able to access current documentation.	Subject identification processes must include, but are not limited to, confirmation of full name as provided on subject report and at least two of the following: 1) date of birth, 2) street address used on application or authorization document, 3) information from the country ID or Tax ID document 4) driver's license number, and 5) report ID number. Auditor will seek evidence of adherence to policies and procedures.
6.8 Document Management			
Organization must have and follow a written record retention and destruction policy which, at a minimum, complies with all applicable law and regulation. The policy must include procedures for situations when a controller has requested the return or destruction of Personal Data.	Organization must provide written policy, procedure, or other written documentation describing organization's record retention and destruction practices.	Organization must present written document retention and destruction policy. Organization must make available the person responsible for document retention and destruction. The policy must include procedures for situations when a controller has requested the return or destruction of Personal Data. If interviewed, this person must demonstrate understanding of retention and destruction requirements and processes as well as process to return information to a controller when requested. Organization must provide evidence of adherence to procedures.	Processes must address both electronic and hard copy records and include: 1) period of retention for subject records, 2) method used to determine record age, 3) processes used for actual record destruction, 4) documentation of record destruction activity, 5) individual responsible for initiating, managing, confirming, and documenting record destruction, organizations are subject to secure destruction through means that are reasonable and appropriate to prevent the unauthorized access to or use of information in a subject report, and 6) procedures to return or destroy information when requested by the controller. Auditor will seek evidence of adherence to policies and procedures.
6.9 Organization Worker Certification			
Organization must have and follow a policy requiring all organization workers to certify in writing they will adhere to the	Organization must provide written policy, procedure, or other written documentation describing how/when	Organization must present written procedure for obtaining organization worker written certification(s)	Certification(s) language must include, but is not limited to, agreement by organization workers to: 1) hold, use, and destroy all client and subject information in a secure manner, 2) provide

confidentiality, security and legal compliance practices of the organization.	organization obtains from all organization workers certification(s) in which worker agrees to adhere to the organization's confidentiality, security, and legal compliance practices and where such certifications are retained. organization must provide copy of certification document(s).	that worker will adhere to organization's confidentiality, security, and legal compliance practices. If questioned, organization workers must confirm they were required to provide this certification(s). Auditor may ask to see, but not retain copy of, certification(s) signed by one or more workers. Organization must provide evidence of adherence to procedures.	subject information to third parties only after following defined authentication procedures, 3) abide by physical security practices, 4) abide by information security practices, and 5) follow all compliance practices of the organization. Auditor will seek evidence of adherence to policies and procedures.
6.10 Professionalism and Proficiency Training			
Organization must have and follow procedures to provide initial and ongoing training to organization workers, where training is commensurate with specific worker role and responsibilities. organization must retain records of such training. Training should also be conducted of organization's sub-contractors. This can either be done by the organization directly or be done as a requirement of the contract in compliance with the organization's requirements and proof of training provided to organization.	Organization must provide written policy, procedure, or other documentation to provide initial and ongoing training to organization workers, where training is commensurate with specific worker role and responsibilities and retain records of such training. Training should also be conducted of organization's sub-contractors. This can either be done by the organization directly or be done as a requirement of the contract in compliance with the organization's requirements and proof of training provided to organization.	Organization must make available to auditor any materials used to train organization workers on specific job responsibilities and records of such training. If interviewed, Organization workers must describe training which was received. Organization must provide evidence of adherence to procedures.	Organization must provide information and training to workers which are specific based on worker role and responsibilities. Organization must provide training on general requirements of confidentiality, professionalism, accuracy, and worker's role as a representative of the organization. Organization must retain records of all such training. Training methods may include, but are not limited to: 1) written material, 2) online training, 3) training classes/webinars, 4) one-on-one training sessions, and/or 5) on-the-job training. Auditor will seek evidence of adherence to policies and procedures.
6.11 Worker Confidentiality, Legal, and Compliance Training			
Organization must have and follow procedures to provide initial and annual training to all workers on confidentiality, security and legal compliance practices of the organization and maintain records of such training. This can either be done by the organization directly or be done as a requirement of the contract in compliance with the organization's requirements.	Organization must provide written policy, procedure, or other documentation which describes the requirement for and methodology used to train organization workers on the confidentiality, security, and legal compliance procedures of the organization and how such records are retained. This can either be done by the organization directly or be done as a requirement of the contract in compliance with the organization's requirements.	Organization must present written procedure for providing initial and annual training to organization workers regarding confidentiality, security, and legal compliance practices of organization and how such records are retained. Organization must make available to auditor any materials used for such training. If interviewed, organization workers must describe training which was received. Organization must provide evidence of adherence to procedures.	Organization must provide initial and annual training to organization workers regarding confidentiality, security, and legal compliance practices by using one or more methods which include, but are not limited to: 1) written material, 2) online training, 3) training classes/webinars, 4) one-on-one training sessions, and/or 5) on-the-job training. organization must retain records of such training. Auditor will seek evidence of adherence to policies and procedures.
6.12 Visitor Security			
Organization must have and follow procedures for a visitor security program to ensure visitors do not view or have unauthorized access to confidential or subject information.	Organization must provide written policy, procedure, or other documentation which describes the visitor security program and how visitors are prevented from viewing or accessing confidential or subject information.	Organization must present written procedure for ensuring visitor security which prevents viewing or accessing of confidential or subject information. Organization must make available the person responsible for visitor security program. This person must be able to describe and/or provide documentation related to visitor security and access	Visitor security policy must include method(s) which prevents visitors from viewing or accessing confidential or subject information. These methods may include, but are not limited to: 1) use of sign in/out registry, 2) issuance of temporary badges, 3) situations in which an organization worker must escort the visitor, 4) controlled access to systems and data, and 5) controlled access to areas of facility in which subject information is readily available on screens or hard copy. Auditor will seek evidence of adherence to policies and procedures.

		control. If questioned, organization workers must demonstrate knowledge of visitor security policy. Organization must provide evidence of adherence to procedures.	

6.13 Responsible Party			
Organization must employ one person designated to oversee and administer the accreditation process and ongoing compliance by the organization, including enforcement of the Accreditation Standard. This person must be vested with the responsibilities and authority attendant to this task, and must be the organization contact for the auditor and accreditation related matters for PBSA.	Organization must employ a minimum of one person who is responsible for organization's accreditation activity and on-going compliance with applicable standards/requirements as evidenced by written job description(s) or other documentation. If multiple people are responsible, one person must hold overall responsibility as evidenced by written job description or other documentation.	Organization must present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for accreditation activity and on-going compliance. organization must make this person available either in person or by phone. If interviewed, organization workers must identify the person(s) that can provide accreditation expertise when needed.	The person responsible for overall accreditation must affirm his/her role as being responsible for accreditation/certification activity and on-going compliance within the organization and that s/he is qualified to hold such responsibility.
6.14 Document Control			
Organization must have and follow procedures for document control and versioning to ensure correct versions of all controlled documents are used.	Organization must provide written policy, procedure, or other documentation describing the methods used to control documents and ensuring correct version of all controlled documents is used.	Organization must present procedures to ensure only the most recent version of any controlled document is used internally and made available externally. Organization must make available the person(s) responsible for document control. If interviewed, organization workers must demonstrate knowledge of document control requirements, describe methods used to ensure document control, must be able to access current copy of documentation, and must identify person(s) responsible for document control systems. Organization must provide evidence of adherence to procedures, including training records.	Organization must provide training to organization workers regarding how to identify, retrieve and use only most current version of any controlled document using 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. Auditor will seek evidence of adherence to policies and procedures, including training records.
6.15 Ethics Reporting			
Organization must have a process by which organization workers can anonymously, to the extent possible and allowable by local law, report ethical, compliance, and work product concerns without fear of identification or retaliation based on such reporting. organization must have and follow a procedure to inform organization workers of reporting process and anonymity; organization must have and follow procedures for investigation of reported concerns.	Organization must provide written policy, procedure, or other documentation describing how/when organization informs organization workers of reporting process, how organization investigates reported concerns, and how organization worker anonymity is maintained. If the organization maintains that anonymous ethics reporting is not allowed by local law, the organization should provide evidence to support this. They should provide information about how they allow organization workers to report ethical concerns.	Organization must present written procedure for informing organization workers of reporting process, availability, investigating reported concerns, protecting anonymity, and prohibiting retaliation based on such reporting. If interviewed, organization workers must demonstrate knowledge of reporting process and be able to access current copy of documentation. organization must provide evidence of adherence to procedures. If the organization maintains that anonymous ethics reporting is not allowed by local law, the organization should provide evidence to support this. They should	Organization must provide information to organization workers regarding availability and use of organization ethics reporting process. Methods to provide information must include at least one of the following: 1) inclusion in organization Worker Handbook, 2) posting in organization worker common area such as breakroom, 3) online training or help system, or 4) one-on-one information sharing. Auditor will seek evidence of adherence to policies and procedures. If the organization maintains that anonymous ethics reporting is not allowed by local law, the organization should provide evidence to support this. They should provide information about how they allow organization workers to report ethical concerns.

		provide information about how they allow organization workers to report ethical concerns.	

work

For purposes of this Standard, the terms and acronyms below have the following definitions.

Note that where clause requirements include "signature" or "signed by" wet or electronic signature shall be deemed to meet signature requirement.

1. **Automated Reporting**: This refers to an inquiry being made, results being returned, and results being placed in a subject report without any manual intervention or review by a person.
2. **Client**: This refers to a purchaser from a background screening company (also referred to as customer or end user.)
3. **Depth of Search**: This refers to the number of years covered by a search. Examples include a 7-year search and 10-year search where record search must cover at least 7 years or 10 years respectively.
4. **Organization Worker/Worker**: Any individual who performs services for organization and who has access to organization premises and/or systems. These terms encompass employees as well as temporary workers, interns, contractors and others who perform work for the organization.
5. **Outsourced Verification Services**: Refers to a business arrangement in which the organization contracts with another company and that company conducts employment, academic, and/or reference checks on behalf of the organization and return results to the organization (see Clause 5.8). Outsourcing criminal record checks to public record field researchers **ARE NOT** considered "Outsourced Verification Services."
6. **Policy**: A written directive that is required to be followed by the entity.
7. **Procedure:** A written description of how a policy is implemented and followed by the entity. (Procedures may be referred to within the entity as standard operating procedures, SOPs, operating guidelines or other names.)
8. **Search Methodology**: Refers to the manner by which the search is conducted. Examples include: hands-on, in-person search (such as when a public access terminal is used at a courthouse), electronic access to original source (such as a remote electronic search of court records), electronic access to commercial database, electronic access to a government database, telephonic inquiry to a source (such as school, employer, or reference) and email inquiry to a source (such as school, employer, or reference).
9. **Subject Information**: Any information about an individual subject provided to the organization by the subject, client, or other parties in the course of compiling a subject report.
10. **Subject Report**: The output of a background investigation conducted by an organization.
11. **Third Party Service Provider (vendor/agent)**: Any person or entity contracted or employed by an organization, other than another organization providing subject reports, who searches for and/or retrieves information that is currently in the custody of a government entity such as a court, agency or other government repository.
12. **Verification**: Academic, employment, reference, and other checks conducted using source information which is not public.