



National Background Screening Accreditation Board

US Employment Screening Company Accreditation Program

Accreditation Standard
Version 1



Section 1: Information Security

Clause 1.1

1.1 Information Security Certification

Entities holding Personally Identifiable Information (PII) must maintain current security certifications or provide evidence of security audits with no unresolved critical vulnerabilities. Certification must be issued by a qualified security assessor.

Clause 1.2

1.2 Information Security Policy

CRAs must implement a written information security policy compliant with applicable laws and designate responsible personnel for its enforcement.

Clause 1.3

1.3 Data Security

CRAs must protect consumer information from unauthorized access, ensuring secure transmission and storage of both electronic and hard copy data.

Clause 1.4

1.4 Intrusion and Data Security

CRAs must have procedures to prevent, detect, investigate, and respond to system intrusions, including consumer and breach notifications as required by law.

Clause 1.5

1.5 Storage and Backup of Data

Data must be securely backed up and stored in an encrypted or protected manner, meeting all legal requirements.

Clause 1.6

1.6 Access Protocol

Secure access protocols must be implemented for CRA workers, clients, and authorized users accessing consumer information.

Clause 1.7

1.7 Electronic Access Control

Access to electronic systems containing consumer information must be controlled, with rights updated as personnel or system changes occur.



Clause 1.8

1.8 Physical Security

Physical access to CRA facilities and data storage areas must be secure and controlled.

Clause 1.9

1.9 Consumer Information Privacy Policy

CRAs must maintain a privacy policy detailing the collection, use, sharing, storage, and destruction of consumer information. This policy must be available on the CRA's website and upon request.

Clause 1.10

1.10 Unauthorized Browsing

CRAs must prohibit workers from accessing files or databases without a legitimate business need.

Clause 1.11

1.11 Record Destruction

Records containing consumer information must be destroyed in compliance with legal requirements, ensuring they are unrecoverable.

Clause 1.12

1.12 Sensitive Data Masking

Sensitive data, such as Social Security Numbers, must be suppressed or truncated as required by law. Full access to sensitive data requires end-user certification of compliance with legal safeguards.

Section 2: Legal and Compliance

Clause 2.1

2.1 Compliance with Law and Regulation

CRAs must comply with all applicable laws and regulations, including the Federal FCRA and those outlined in this standard.

Clause 2.2

2.2 Federal Consumer Reporting Law

CRAs must designate personnel responsible for compliance with federal FCRA provisions related to employment consumer reports.

Clause 2.3

2.3 State Consumer Reporting Laws

CRAs must designate personnel responsible for compliance with state consumer reporting laws.

**Clause 2.4****2.4 Driver Privacy Protection Act (DPPA)**

CRAs must designate personnel responsible for compliance with DPPA requirements for consumer reports containing DPPA-regulated information.

Clause 2.5**2.5 State Implemented DPPA Compliance**

CRAs must designate personnel responsible for compliance with state-specific DPPA implementations.

Clause 2.6**2.6 Integrity**

CRAs must maintain a policy prohibiting bribery or fraudulent activities to gain preferential treatment from public officials or government entities.

Clause 2.7**2.7 Prescribed Notices**

CRAs must provide clients with current versions of all required federal notices under the FCRA, such as those prescribed by the Consumer Financial Protection Bureau.

Clause 2.8**2.8 Agreement from Client**

CRAs must obtain signed agreements from clients, ensuring compliance with applicable laws, including the federal FCRA and applicable state laws.

Clause 2.9**2.9 Client Legal Responsibilities**

CRAs must inform clients of their legal responsibilities when using consumer reports and recommend consulting legal counsel for compliance.

Clause 2.10**2.10 Client Required Documents**

CRAs must inform clients of necessary forms or documents required for specific searches.

Clause 2.11**2.11 Disclosure and Authorization**

CRAs must inform clients of legal requirements for disclosing and obtaining consumer authorization before requesting reports.



Clause 2.12

2.12 Adverse Action

CRAs must inform clients of legal requirements for taking adverse action based on consumer reports and recommend consulting legal counsel for compliance.

Clause 2.13

2.13 Consumer Disputes

CRAs must have procedures for handling and documenting consumer disputes in compliance with all federal, state and local legal requirements.

Clause 2.14

2.14 Database Criminal Records

When reporting public record information which is likely to have an adverse effect on a consumer's ability to obtain employment, the CRA shall comply with Section 613 of the FCRA. Specifically, regarding database records, the CRA shall never report the database record but shall verify the information with a county or statewide criminal search and only report information derived from this verification search.

Clause 2.15

2.15 Identification Confirmation

CRAs must ensure maximum accuracy when verifying consumer identity before reporting information on the consumer.

Clause 2.16

2.16 Full File Disclosure

CRAs must have a policy to document and respond to consumer requests for all information in their file.

Clause 2.17

2.17 Jurisdictional Knowledge

CRAs must employ or access qualified personnel to understand court terminology and jurisdictional differences when reporting court records.

Clause 2.18

2.18 Automated Reporting Systems

CRAs using automated systems must ensure that reported results accurately reflect source information.

Clause 2.19

2.19 Quality

CRAs must maintain procedures to ensure the accuracy, completeness, and quality of all work products, especially public records with potential adverse effects.



Clause 2.20

2.20 Reappearance of Inaccurate Information

The CRA must establish and follow documented procedures designed to prevent the reappearance of previously corrected or inaccurate consumer information in any consumer report.

Clause 2.21

2.21 Quality Analysis

The CRA must maintain and follow procedures to regularly audit and evaluate product quality. All identified quality issues, including those arising from consumer disputes, must be quantified, analyzed for root cause, and addressed through documented corrective actions.

Section 3: Client Education

Clause 3.1

3.1 Truth in Advertising

The CRA must have and follow a procedure to clearly communicate to clients the original data sources (e.g., county or state records, employers, academic institutions), inherent limitations, and variables that may affect the availability, accuracy, and scope of information provided in each consumer reporting product.

Clause 3.2

3.2 Legal Counsel

The CRA must have and follow a procedure to inform clients that it is not a provider of legal advice. Clients must be advised to consult their own legal counsel to ensure that their employment screening policies and practices comply with all applicable laws and regulations.

Clause 3.3

3.3 Understanding Consumer Reports

The CRA must maintain and follow a procedure to guide clients on how to properly order, retrieve, interpret, and understand the information contained in consumer reports.

Clause 3.4

3.4 Information Protection

The CRA must have and follow a procedure to inform clients about:

1. The sensitive and confidential nature of consumer reports;
2. Their legal obligation to safeguard such information; and
3. Proper retention and destruction practices as required by the FCRA and DPPA.

Section 4: Researcher and Data Standards

Clause 4.1

4.1 Public Record Researcher Agreement

The CRA must have and follow a procedure requiring all non-employee public record researchers to sign a formal agreement (including any amendments or addenda). The agreement must clearly define the scope of services, jurisdictions covered, research methodology, verification practices, disclosure and communication standards, confidentiality obligations, and compliance with FCRA requirements.



Clause 4.2

4.2 Vetting Requirement

The CRA must maintain and follow procedures to thoroughly vet and approve all new public record researchers before engagement.

Clause 4.3

4.3 Public Record Researcher Certification

The CRA must have and follow a procedure requiring researchers to certify in writing that they will:

1. Conduct research in full compliance with applicable legal and regulatory requirements;
2. Use only official record repositories;
3. Never obtain information through unlawful or unethical means; and
4. Dispose of consumer information in accordance with FCRA requirements.

Clause 4.4

4.4 Errors and Omissions Coverage (E&O)

The CRA must obtain proof of Errors and Omissions insurance from each public record researcher. If a researcher cannot provide proof, the CRA must maintain coverage to protect against uninsured or underinsured researchers.

Clause 4.5

4.5 Information Security

The CRA must implement secure methods for transmitting orders and receiving search results from public record researchers.

Clause 4.6

4.6 Auditing Procedures

The CRA must have and follow a procedure to periodically audit all active public record researchers to ensure ongoing quality and compliance.

Section 5: Verification Services Standards

Clause 5.1

5.1 Verification Accuracy

The CRA must maintain reasonable procedures to ensure the maximum possible accuracy when obtaining, documenting, and reporting verification information.

Clause 5.2

5.2 Current Employment

The CRA may contact a consumer's current employer only when specifically authorized by the consumer, or when such authorization has been obtained by the client and provided to the CRA.



Clause 5.3

5.3 Procedural Disclosures

The CRA must provide full disclosure to clients regarding general verification practices, including:

1. The number and definition of verification attempts;
2. Applicable locate or third-party fees; and
3. Standard question formats used during verification.

Clause 5.4

5.4 Verification Databases

If the CRA compiles or resells stored employment or education verification data, it must maintain procedures to ensure data accuracy and to properly handle consumer disputes.

Clause 5.5

5.5 Use of Stored Data

When providing investigative consumer reports from stored data, the CRA must not report adverse information unless it has been reverified within the past three months or a shorter period if required by law.

Clause 5.6

5.6 Documentation of Verification Attempts

The CRA must maintain procedures to document all verification attempts and their outcomes for every completed verification service.

Clause 5.7

5.7 Outsourced Verification Services

The CRA must require signed agreements from all outsourced verification providers. Agreements must clearly define service scope, methodology, documentation standards, disclosure requirements, completion timelines, confidentiality obligations, reinvestigation procedures, and compliance with FCRA responsibilities.

Clause 5.8

5.8 Conflicting Data

If the CRA receives new or conflicting verification information within 120 days (or as required by law) of an original report, it must have procedures to promptly notify the client of the updated information.

Clause 5.9

5.9 Authorized Recipient

When verification requests are made via phone, fax, email, or mail, the CRA must have and follow procedures to ensure the request is sent only to an authorized recipient.



Section 6: Business Practices

Clause 6.1

6.1 Background Checks for CRA Personnel Charged with Enforcement of Policy

The CRA must have and follow a policy requiring criminal background checks and government sanction list checks for all owners, officers, principals, and personnel responsible for enforcing company policy. These checks must:

1. Cover at least seven years of residential history;
2. Be repeated every two years;
3. Be retained in accordance with applicable law; and
4. Be evaluated based on the “Green Factors” — nature of offense, time elapsed, and relevance to role.

Clause 6.2

6.2 Background checks for CRA Workers

The CRA must conduct criminal background and sanction checks on all personnel every two years. Evaluations must apply the same “Green Factors” to determine continued eligibility for employment.

Clause 6.3

6.3 Changing Law and Regulation

The CRA must designate an individual or team responsible for monitoring and ensuring compliance with all applicable laws and regulatory changes, or must retain an external expert for this purpose.

Clause 6.4

6.4 Insurance

The CRA must maintain at least \$1 million in Errors and Omissions insurance, or self-insure in compliance with applicable state insurance requirements.

Clause 6.5

6.5 Client Authentication

The CRA must verify and document the identity and qualification of every client before providing consumer information. Written records must be maintained for all authorized clients.

Clause 6.6

6.6 Vendor Authentication

The CRA must verify and document the identity and qualification of all vendors before sharing consumer information, and maintain written records of all vendor authorizations.

**Clause 6.7****6.7 Consumer Authentication**

Before releasing information to a consumer via telephone, the CRA must implement reasonable procedures to verify the consumer's identity and maintain documentation of the verification process.

Clause 6.8**6.8 Document Management**

The CRA must maintain and follow a written record retention and destruction policy compliant with all applicable laws and regulations.

Clause 6.9**6.9 Employee Certification**

All CRA workers must sign a written certification agreeing to adhere to the CRA's confidentiality, security, and legal compliance requirements.

Clause 6.10**6.10 Professionalism and Proficiency Training**

The CRA must provide initial and ongoing training appropriate to each worker's role and responsibilities, and maintain records of such training.

Clause 6.11**6.11 Worker Confidentiality, Legal, and Compliance Training**

All CRA workers must receive initial and annual training covering confidentiality, data security, and legal compliance. Training records must be retained.

Clause 6.12**6.12 Visitor Security**

The CRA must implement visitor management procedures to prevent unauthorized access to consumer information.

Clause 6.13**6.13 Responsible Party**

The CRA must designate a qualified individual responsible for managing accreditation, enforcing compliance, and serving as the primary contact for auditors and accreditation authorities.

Clause 6.14**6.14 Document Control**

The CRA must maintain procedures for document control and version management to ensure that only current, approved versions of controlled documents are in use.

Clause 6.15**6.15 Ethics Reporting**

The CRA must provide an anonymous reporting mechanism that allows workers to report ethical, compliance, or work-quality concerns without fear of retaliation. Procedures must ensure employee awareness, protect anonymity to the extent possible, and include investigation and resolution processes.