NAPBS PROVIDER
DATA SECURITY & PRIVACY GUIDELINES

Statement of Purpose[1]

Consumer Reporting Agencies and their supporting information and service providers are routinely entrusted with **PII** on individual consumers in the course of providing services to their clients. Accordingly the purpose of this document is to establish minimum guidelines that **NAPBS Providers** should follow in order to protect such PII from unlawful or unethical use.

Application of Appropriate Laws

This document is intended to provide uniform minimum guidelines for NAPBS Providers. The National Association of Professional Background Screeners recognizes that certain laws may require stricter standards than those described herein, and accordingly NAPBS Providers must perform data security and privacy measures in accordance with any applicable law local to their jurisdiction. Where such local law calls for a lower level of protection than that established by these Guidelines, the requirements of these Guidelines shall apply.

Principles

1) NAPBS Providers shall, in accordance with these Guidelines, exercise appropriate due diligence when handling PII in the course of providing services to their clients, recognizing that unauthorized access to or misuse of PII can cause harm to **consumers**.

2) The Provider mush employ any security and protection measures (e.g., physical security devices, **encryption** and access restrictions) appropriate to the nature of the category of PII they are handling and the risk associated with its intended use.

3) PII will be processed in accordance with applicable law and Guidelines promulgated by the NAPBS.

4) The Provider shall collect PII for specific, legitimate purposes and not process it in any additional manner incompatible with those purposes.

5) PII should be retained only as long as necessary for the purposes it was collected and processed for, and/or as required by federal, state or local law.

6) PII shall be processed in accordance with the individual's legal rights, as described in these Guidelines or as provided by law.

7) Appropriate technical, physical, and organizational measures will be taken to prevent unauthorized access, unlawful processing and unauthorized or accidental loss of PII.

[1] Key terms are **bolded** on their initial appearance and defined in the *Glossary*.

General Guidelines

8) The task of protection of PII shall be divided into four general subject areas:

- Policy and Procedural Measures
- Infrastructure Measures
- PII Transmission Protective Measures
- Security Response Measures

a) It is intended that the implementation of these Guidelines be flexible and scalable based upon the size and complexity of the Provider's organization. The Provider should implement safeguards appropriate to their organizational size, structure and specific circumstances. For example, some Providers may choose to describe their safeguard programs in a single document, while a larger Provider may detail their plans in several different documents, such as one to cover an information technology division, another to describe their training program for employees, et cetera. Similarly a Provider may decide to designate a single employee to coordinate safeguards, or spread this responsibility among several employees who will work together on it.

b) In addition, a Provider with small number of staff may design and implement a more limited employee training program than one with a large number of employees. Or a Provider with no employees would simply assume any responsibility themselves for securing the PII they handle. A Provider who does not receive or store any PII online may take fewer steps to assess risks to their computers than one who routinely conducts business online.

Policy and Procedural Measures

9) Policy and Procedural Measures can be categorized further as *Organizational Accountability*, *Employee Management and Training*, and *Formalized Procedures*, described as follows:

a) *Organizational Accountability*

1) Providers should designate one or more members of their staff with the responsibility to protect PII.

2) Providers should perform a background check prior to hiring any staff that will have access to PII.

3) Providers should establish a formal process to identify and credential prospective clients before allowing access to reports that may contain PII from non-public data sources. Providers should consider the following in the credentialing process:

i) A completed subscriber / membership application;

ii) Articles of Incorporation / current business license;

iii) Certification of Compliance and **FCRA** Permissible Use;

iv) Verification of Location;

v) Adherence to *NAPBS Provider Data Privacy & Security Guidelines*

b) *Employee Management and Training*

1) Providers with employees should conduct training regarding the lawful and intended purposes of processing PII; the need to protect and keep PII accurate and up-to-

date; and the need to maintain the confidentiality of any PII employees may have access to.

c) *Formalized Procedures*

1) Provider should develop a written plan that describes their program to protect PII. The plan must be appropriate to their company's size and complexity, the nature and scope of its activities, and the sensitivity of the information it handles.

Infrastructure Protective Measures

10) Infrastructure Protective Measures can be further categorized as *Physical Security*, *Document Retention* and *Information Systems Security,* described as follows:

a) *Physical Security*

1) Ideally Providers should employ a "triple lock and key" approach to storing physical records containing PII. Specifically:

i) Providers shall employ physical measures to protect the perimeter of all buildings and facilities housing PII. Minimum acceptable measures shall include "lock and key" protection on all doors, windows and any other potential points of entry to the storage location. Additional perimeter security measures, such as an electronic security system to detect intrusion and unauthorized access, are highly recommended.

ii) PII shall preferably be housed within a separately-defined physical space within the area defined above, such as an interior room that is capable of being locked. Keys to this area shall be issued only to those individuals with a legitimate business need to access PII.

iii) PII shall preferably be stored in a device capable of being locked, such as a locking file cabinet, within the space defined above. Keys to the storage device shall be issued only to those individuals with a legitimate business need to access PII.

b) *Document Retention*

1) Providers shall develop a Document Retention Policy whereby PII are securely retained for the time period necessary to comply with any applicable laws, respond to audit requests by clients and other authorized entities, and fulfill FCRA disclosure requests by individual consumers.

2) Upon expiration of the time period set forth in the Information Provider's Document Retention Policy, **Sensitive Records** shall be disposed of in accordance with regulations promulgated by the Federal Trade Commission regarding the disposal of **consumer report** information and records.[1] The FTC regulations do not mandate *specific* disposal methods, however shredding or burning paper records containing PII are given in the footnoted material as examples of measures that would generally be appropriate.

c) *Information Systems Security*

1) Computer equipment housing Sensitive Records stored electronically shall be located in a physically secure area as defined in the *Physical Security* section above.

---

[1] 16 C.F.R. Part 682. (http://www.ftc.gov/opa/2004/11/factadisposal.htm); (http://www.ftc.gov/os/2004/11/041118disposalfrn.pdf)

2) Physical access to computer equipment housing Sensitive Records shall be limited to personnel with a legitimate business need.

3) Computer equipment shall run software (operating system-based or otherwise) which requires users to authenticate themselves, through entry of a **Strong Password**, prior to gaining access to Sensitive Records stored electronically.

4) Each individual authorized user should be issued separate logon credentials to enable usage tracking and to establish an audit history.

5) Sensitive Records housed on computer equipment connected to a hardwired **Local Area Network (LAN)** shall be further protected from unauthorized access by other devices on the LAN, requiring authentication using a Strong Password prior to granting access across the LAN.

6) Due to their "open" nature and greater susceptibility to unauthorized access, the use of wireless LAN networking equipment to connect electronic devices housing Sensitive Records requires careful attention. In situations where they are utilized, wireless LAN networking equipment (802.11a/b/g, etc.) shall minimally utilize the 128-bit **Wired Equivalent Privacy (WEP)** security protocol. Additional levels of security are strongly recommended if employing wireless LAN networking equipment.

7) Computer equipment connecting to outside networks and/or the Internet shall be isolated using hardware and/or software-based firewalls to protect against unauthorized intrusions from users "outside of" the physically-protected space.

8) Providers shall protect their computer equipment from **malware** using up-to-date software and/or hardware solutions designed to protect against such attacks.

Data Transmission Protective Measures

11) Providers shall strive to ensure a consistent and adequate level of protection for PII processed and/or transferred amongst Providers. A data transfer shall be carried out only if applicable legal requirements are met, and if:

- The transfer is based on a clear business need;
- The receiving entity provides appropriate security for the data as outlined in these guidelines;
- The receiving entity ensures compliance with these Guidelines for the transfer and any subsequent processing and/or storage.

12) At times Providers may be required to transfer PII to selected external third parties they have hired to perform screening-related services on their behalf. Such third parties may process the PII in accordance with the Provider's specific instructions, or make decisions regarding the PII as part of the delivery of their services. In either case the Provider shall select reliable suppliers who undertake, by contract or other legally binding and permissible means, to put in place appropriate security measures to ensure an adequate level of protection. Specifically:

a) Providers shall require external third-party suppliers to comply with these Guidelines, and otherwise guarantee comparable levels of protection required of Providers in handling PII.

b) Such selected third parties will have access to PII solely for the purposes of performing the services specified in the applicable service contract.

c) If a Provider concludes that a supplier is not complying with these obligations they shall act promptly and effectively to remedy the situation.

13) Providers shall exercise due diligence when transmitting PII via the Internet or other public or insecure networks. Security measures to be considered for its transmission should include:

a) **Secure Sockets Layer (SSL)** or other secure connection so that the information is encrypted in transit;

b) **IP address** filtering to permit connections only with or from authorized locations;

c) Port filtering to permit connections only to authorized ports;

d) Access Logs to provide an audit trail of activity;

e) Credential based access to system integration points;

f) Protective measures when sending PII via e-mail;

g) E-mail containing PII should be encrypted from the sender to the receiver;

h) If PII is transmitted in an un-encrypted manner, the PII should be obscured. Examples include:

- Dates of birth shall be transmitted using only the month and year, with the day obscured;
- Social Security Numbers shall be transmitted with all but the last four digits obscured.

Security Response Measures

14) Providers should recognize that data privacy and security is a fluid environment and that prevention, detection and response to attacks, intrusions or other system failures are an important component to protecting PII. Accordingly Providers should have the following components in place:

a) A documented contingency plan to address any breaches of their physical, administrative or technical safeguards;

b) A central point of contact for their staff to report and receive updates about any security risks or breaches;

c) A document addressing when and how customers will be notified if their non-public PII is subject to loss, damage or unauthorized access that could result in possible significant harm.

15) Additionally Providers should consider the following measures in their data security and privacy plan:

a) Steps to preserve the security, confidentiality and integrity of PII in the event of a computer or other technological failure. For example, back up all customer data regularly.

b) Audit trails to track how, where, when and who accessed Sensitive Records.

c) Regularly review the plans, procedures and effectiveness of the company's data privacy and security measures, and adjust in light of relevant circumstances, including changes in business arrangements or operations, the results of testing and monitoring of safeguards, et cetera.

Glossary[1]

Consumer Reporting Agency (CRA): Any person or group which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating *consumer* credit information or other information on consumers for the purpose of furnishing *Consumer Reports* to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing Consumer Reports.

Consumer: Individuals who purchase, use, maintain, and dispose of products and services. A member of that broad class of people who are affected by pricing policies, financing practices, quality of goods and services, credit reporting, debt collection, and other trade practices for which state and federal consumer protection laws are enacted.

Consumer Report: A consumer report, for our purposes, is typically a pre-employment or pre-tenancy background report, prepared by a *Consumer Reporting Agency* on a *consumer*.

Credentialing: The process of obtaining and reviewing documentation (licensure, certifications, insurance, et cetera) provided by individuals, businesses or organizations. Generally this will include reviewing the information provided by the source and verifying that the information is accurate and complete.

Cryptography: A field of mathematics and computer science concerned with information security and related issues, particularly *encryption* and authentication.

Cryptographic protocol: an abstract or concrete *protocol* that performs a security-related function and applies *cryptographic* methods. Cryptographic protocols are widely used for secure application-level data transport

Encryption: The act of fact of converting computer data and messages to something incomprehensible by means of a key, so that it can be reconverted only by and authorized recipient holding the matching key.

FCRA: (Federal) Fair Credit Reporting Act: The federal law that regulates entities who are in the business of providing reports on consumers' credit standing, character and reputation (*consumer reports*). It should be noted that the Act has been expanded to regulate not only credit reports, as the name would suggest, but information derived from public records associated with consumers' criminal records and civil litigation histories as well. (In fact it would be more appropriately named the Fair Credit and Employment Reporting Act.)

IP address: In computer networking, an IP address (internet protocol address) is a unique number that devices use in order to identify and communicate with each other on a network. Any participating network device—including routers, computers, printers, internet fax machines, et cetera—must have its own unique IP address. The uniqueness of IP addresses makes it possible in many situations to track which computer has sent a message or engaged in some other activity on the Internet.

Local Area Network (LAN): A computer network covering a small local area, such as a home, office or small group of buildings.

Malware: Short for "malicious software": software designed to infiltrate or damage a computer system without the owner's consent, commonly taken to include computer viruses, Trojan horses, spyware and adware.

---

[1] Any italicized words which appear within a definition are defined in this glossary.

NAPBS Provider(s): Providers who provide information or services to the background screening industry, including, but not limited to: Employment & Education Verification Providers; Application Service Providers; Software Providers; Credit Report Providers; Data Base Providers; Motor Vehicle Report Providers; and International, National, Regional and Local Wholesale Research Providers as defined in the *NAPBS Criminal Research Provider Guidelines*.

PII: Personally Identifiable Information, or Personally Identifying Information: any pieces of information which can potentially be used to uniquely identify, contact, or locate a single person. PII can also be exploited by criminals to steal the identity of a person.

Protocol: In computing, a **protocol** is a convention or standard that controls or enables the connection, communication, and data transfer between two computing endpoints. Protocols may be implemented by hardware, software, or a combination of the two. At the lowest level, a protocol defines the behavior of a hardware connection.

Secure Sockets Layer (**SSL):** a *cryptographic protocol* which provides secure communications on the Internet.

Sensitive Records: media in any form (paper, electronic or otherwise) containing *PII*.

Strong Password: a password that is difficult to detect by both humans and computer programs, effectively protecting data from unauthorized access. A strong password consists of at least six characters (and the more characters, the stronger the password) that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed, and is typically case-sensitive, so a strong password contains letters in both uppercase and lowercase. Strong passwords also do not contain words that can be found in a dictionary or parts of the user's own name.[1]

Transmission: in the context of these Guidelines, the passing of PII from one point to another by electronic means.

Wired Equivalent Privacy (WEP): A scheme to secure wireless networks (WiFi). Because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping. WEP was intended to provide comparable confidentiality to a traditional wired network, hence the name. Several serious weaknesses were identified by cryptanalysts, and WEP was superseded by WiFi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004. Despite the weaknesses, WEP provides a level of security that can deter casual snooping.

[1] Definition of "Strong Password" taken from Webopedia.com (http://isp.webopedia.com/TERM/S/strong_password.html),