## System access and security policy

NAPS Background Checks data service shall provide access to customer through computer software, XML Integration, Internet web browser, e-mail, telephone, fax or hard copy. Customer agrees to carry out the following in order to preserve the security of the Services being provided.

1. To take appropriate measures so as to protect against the misuse and/or unauthorized access of our services through any methods, including unauthorized access through or to Customer's user identification numbers or passwords ("Account ID's"). Such misuse or unauthorized access shall include any disclosure, release; viewing or other unauthorized access to information such as social security numbers, driver's license numbers or dates of birth. Customer agrees that NAPS may temporarily suspend Customer's access for up to ten (10) business days pending an investigation of Customer's use or access. Customer agrees to cooperate fully with any and all investigations. If any misuse or unauthorized access is found, NAPS may immediately terminate this Agreement without notice or liability of any kind.

2. The ability to access data shall be restricted to only duly authorized personnel, whether by computer and/or Internet-based systems or otherwise, all according to procedures that meet or exceed all applicable regulations including, but not limited to, the FCRA, other applicable federal, state and local laws, statutes, regulations, rules and court orders. NAPS shall take commercially reasonable measures to maintain the accessibility of its services via Internet 24 hours a day, except for such down time as necessary or advisable for upgrade or maintenance. NAPS shall not be responsible for establishing or maintaining Customer's access to the Internet.

3. Customer is hereby notified of the inherent risks associated with all delivery methods of NAPS. Any system or device of any kind used to obtain or receive data services shall be placed in a secure location within customer's facility, and customer shall take all necessary precautions to secure any such system or device in such a manner as to prevent unauthorized access. All such systems or devices shall be disabled or locked after normal business hours or when left unattended by authorized personnel.

4. Each user of Customer's system to access data services will be assigned a unique logon password. Customer shall protect account numbers and passwords used to access data services in such a way as to be known only to authorized personnel, and under no circumstances will unauthorized personnel have knowledge of any such account numbers or passwords. Customer shall instruct each of Customer's users to change their password every ninety days to ensure unauthorized access. Customer shall not post in any manner, passwords or account numbers within customer's facility. Customer further agrees that account numbers and passwords are not to be discussed by telephone to any unknown caller, even if the caller claims to be an employee of NAPS and/or its Affiliates, until such time that verified identification is made by NAPS. Customer shall manage all Account ID's, and notify NAPS promptly if any Account ID becomes inactive or invalid.

5. Any system access software the Customer may use, whether developed by NAPS and/or its Affiliates or provided by a third party vendor, must have account numbers and passwords "hidden" or embedded so that the passwords and account numbers are known only to supervisory personnel or other personnel authorized to use NAPS's services.

6. Customer is responsible for the security of assigned codes, and is hereby notified of the possibility of theft or other form of compromise of Customer's assigned codes, which may or may not be detected, and of the possibility of use of a stolen or compromised assigned code to forge Customer's access to data from NAPS.

7. In the event of a breach of system security or an unauthorized access of Consumer Report information, Customer shall comply with all notice requirements in every jurisdiction where such notice is required and shall provide immediate notice to NAPS, time being of the essence. Upon discovery of a security breach, further access of NAPS's products will be disabled until the breach is secured and further measures are in place to ensure ongoing compliance.

8. Customer specifically acknowledges and agrees that it shall be responsible in all respects for any and all access of services performed as a result of any use of Customer's assigned access codes, whether or not intended or authorized.

9. NAPS may, from time to time, notify Customer of additional updated or new requirements, compliance with which will be a condition of NAPS's continued provision of data services to Customer.

10. NAPS shall have the right to audit Customer to ensure compliance. Customer shall provide NAPS full cooperation and will be responsible for assuring full cooperation of its employees in connection with such audits. Customer will provide NAPS, or obtain for NAPS, access to such properties, records and personnel as NAPS may reasonably require for such purpose.