NATIONAL ASSOCIATION OF STATE CONTRACTORS LICENSING AGENCIES SECURITY AND CONFIDENTIALITY STATEMENT

I, _____, _____, a representative of
First & Last Name Title
the _____,
State Agency Name
acknowledge that I have been granted access to certain National Association of State Contractors Licensing Agencies ("NASCLA") information systems resources, which may include, but are not limited to, secure file transfer protocol (SFTP), and/or related systems/files. This Security and Confidentiality Statement (this "Statement") applies to all confidential information that is retrieved, recorded, transmitted, stored, and/or processed manually or electronically through NASCLA's information systems and network. I further acknowledge the data contained in, and accessed using, NASCLA's information systems, shall remain confidential. Accordingly, NASCLA system users that store NASCLA's "Confidential Information" (as such phrase is defined below) must meet the specific security safeguard requirements outlined in this Statement and agree to abide by the same.

Confidential Information Definition:

Confidential Information is defined as any proprietary or non-public information, received from NASCLA or another party in relation to your relationship with NASCLA. Confidential Information may be received in a variety of media, including electronic, written and verbal. Information is deemed Confidential Information regardless of whether it is explicitly labeled as such at the time of disclosure. Confidential Information includes all "Personal Data" (as that phrase is defined below). Personal Data means information related to an identified or identifiable person and includes, but is not limited to: a person's social security or other identifying information, such as the NASCLA Accredited Examination score information; driver license information.

Confidential Data Security Safeguards:

Users of NASCLA's systems that store or process NASCLA's Confidential Information are required to maintain an appropriate level of security for the devices that are accessing the NASCLA systems, which includes routine patching of their operating systems and web browsers as suggested by the operating systems creators and the installation of a commercially reasonable active antivirus product to help reduce the threat of malware.

I agree NOT to share my NASCLA login IDs and/or passwords with any other persons, including co-workers, family, external or internal resources. Furthermore, I agree that if under any circumstance I am required to share my NASCLA login ID/password for troubleshooting purposes, I will change my password immediately upon correction of the problem(s).

I understand it is my responsibility to protect NASCLA Confidential Information and NASCLA information systems and networks from tangible and intangible destruction, unauthorized access, or disclosure. I agree to take all precautions to ensure protection, confidentiality, and security of NASCLA Confidential Information and any related resources. As a result, I shall not discuss, disclose, modify, provide, or otherwise make available, in whole or in part, such NASCLA Confidential Information unless authorized for specific business purposes by NASCLA.

I also agree my obligation is to maintain the confidentiality and security of all NASCLA Confidential Information prior to, during, and indefinitely after the termination of any agreement, relationship, and/or employment with my current employer and immediately report any suspicious activity, breach, potential breach, security system breach, security incident, or a potential breach of security related to my access to NASCLA's systems or applications. Additionally, I understand that my access to any/all NASCLA information/resources will be revoked upon termination of my employment or upon authorization by appropriate NASCLA personnel.

If a breach, or potential breach is reported, NASCLA will commence an investigation within twenty-four (24) hours of being notified and determine as quickly as possible the breach or potential breach. I agree to fully cooperate with NASCLA's investigation to greatest extent possible at no cost to NASCLA.

The initial term of this Security / Confidentiality Statement shall be one (1) year commencing as of the date hereof. Thereafter, the term of this Security / Confidentiality Statement shall automatically renew for successive one (1) year terms unless one party provides written notice to the other party at least thirty (30) days in advance of the end of the then existing term that such party does not wish to renew the term of this Security / Confidentiality Statement.

By signing this Security / Confidentiality Statement, I acknowledge the following: (i) I have read and I understand this document; (ii) I will comply with the security policies set by NASCLA; (iii) I understand the consequences of violating said policies and this Security / Confidentiality Statement, up to and including termination of access to NASCLA systems; and (iv) I agree to be bound by applicable requirements and contractual obligations set forth in this Security / Confidentiality Statement.

Signature: _____ Date: _____

Email: _____ Direct Ph # _____

Please email a signed copy to Kirsten Zacharias, NASCLA Strategy Director
Email: kirsten@nascla.org