NH Hicks Written Information Security Program

1. **Policy Statement**

   NH Hicks Written information Security Program (WISP) is intended as a set of comprehensive guidelines and policies designed to safeguard all sensitive data maintained by NH Hicks ("Company"), and to comply with applicable laws and regulations on the protection of Personal Information, found on records and in systems owned by the Company.

2. **Purpose**

   The purpose of this document is to:

   - Establish a comprehensive information security program for NH Hicks with policies designed to safeguard sensitive data that is maintained by the Company, in compliance with federal and state laws and regulations;
   - Establish employee responsibilities in safeguarding data according to its classification level; and
   - Establish administrative, technical and physical safeguards to ensure the security of sensitive data.

3. **Scope**

   This Program applies to all NH Hicks employees, whether full or part-time, including administrative staff, contracted and temporary workers, hired consultants, interns and student employees. The data covered by the Program includes any information stored, accessed or collected at the Company or for the Company.

4. **Policy**

   4.1 Responsibilities

   All employees of the Company are responsible for maintaining the privacy and integrity of all sensitive data as defined above, and must protect the data from unauthorized use, access, disclosure or alteration. All employees of the Company are required to access, store and maintain records containing sensitive data in compliance with this Program.

   4.2 Identification and Assessment of Risks to Company Information

   NH Hicks recognizes that it has both internal and external risks to the privacy and integrity of Company information. These risks include, but are not limited to:

   - Unauthorized access of Confidential data by someone other than the owner of such data

- Compromised system security as a result of a system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of confidential data by employees
- Unauthorized requests for confidential data
- Unauthorized access through hard copy files or reports
- Unauthorized transfer of confidential data through third parties

NH Hicks recognizes that this may not be a complete list of the risks associated with the protection of confidential data. Since technology growth is not static, new risks are created regularly. Accordingly, NH Hicks will actively participate and monitor advisory groups for identification of new risks.

NH Hicks believes the Company's current safeguards are reasonable and are sufficient to provide security and confidentiality to confidential data maintained by the Company. Additionally, theses safeguards protect against currently anticipated threats or hazards to the integrity of such information.

4.3 Policies for Safeguarding Confidential Data

To protect confidential data, the following policies and procedures have been developed that relate to protection, access, storage, transportation, and destruction of records, computer system safeguard, and training.

Access

- Only those employees or authorized third parties requiring access to confidential data in the regular course of their duties are granted access to confidential data, including both physical and electronic records.
- Computer and network access passwords are disabled upon termination of employment or relationship with NH Hicks.
- Upon termination of employment or relationship with NH Hicks, physical access to documents or other recourses containing Confidential data is immediately prevented.

Storage

- Employees of the company will not store confidential data on laptops or on other mobile devices (e.g., flash drives, smart phones, external hard drives). In rate cases where it is necessary to transport confidential data electronically, the mobile device containing the data must be encrypted.

- To the extent possible, making sure that all confidential data is stored only on secure servers maintained by the Company and not on local machines, unsecure servers, or portable devices.
- Paper records containing confidential data must be kept in locked files or other secured areas when not in use.
- Electronic records containing confidential data must be stored on secured servers, and when stored on authorized desktop computers, must be password protected.

Destruction of Confidential Data

- Paper and electronic records containing confidential data must be destroyed in a manner that prevents recovery of the data.
- The Company will take reasonable steps to destroy, or arrange for the destruction of a confidential data within its custody or control containing Personal Information ("PI") which is no longer to be retained by the company by (1) shredding, (2) erasing, or (3) otherwise modifying the PI in those records to make it unreadable or undecipherable through any means.

4.4 Computer System Safeguards

The Company monitors and assesses information safeguards on an ongoing basis to determine when enhancements are required. The Company has implemented the following to combat external risk and secure their network and data containing PI:

- Secure user authentication protocols.
- Unique passwords are required for all user accounts; each employee receives an individual user account.
- Server accounts are locked after multiple unsuccessful password attempts.
- Computer access passwords are disabled upon an employee's termination.
- User passwords are stored in an encrypted format; root passwords are only accessibly by system administrators.
- Secure access control measures.
- Access to specific files or databases containing PI is limited to those employees who require such access in the normal course of their duties.
- Files containing PI transmitted outside the NH Hicks network are to be encrypted.
- The Company performs regular internal network security audits to all server and computer system logs to discover to the extent reasonably feasible possible electronic security breaches, and to monitor the system for possible unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of PI.

- All company–owned computers and servers are firewall protected and regularly monitored.
- Antivirus and anti-malware software are installed and kept updated on all servers and workstations. Virus definition updates are installed on a regular basis, and the entire system is tested and checked at least once per month.

4.5 Reporting Attempted or Actual Breaches of Security

Any incident of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of PI, or of breach or attempted breach of the information safeguards adopted under this Program, must be reported immediately to the Information Security Officer (ISO).

ISO is charged with the identification of all data security incidents where the loss, theft, unauthorized access, or other exposure of sensitive company data is suspected. The ISO reports any such incidents to the CFO. The CFO is responsible for determining appropriate actions in their response to the breach. The ISO will document all breaches and subsequent responsive actions taken. All related documentation will be stored in the Finance Office.

5. Effective Date

This Written Information Security Program was implemented November 1, 2010 and revised January 4, 2014. The Company will review this Program at least annually and reserves the right to change, modify, or otherwise alter this Program at its sole discretion and at any time as it deems circumstances warrant.