Policies and Procedures

Best Practice #3: Privacy and Information Security (NPI)

Purpose	Document a privacy and information security program (policies and procedures) to help ensure Aries Title, Inc. maintains written protocols for the protection of data and Non-public Personal Information (NPI).
Scope	These policies and procedures are for all of Aries Title, Inc. (hereafter referred to as "The Company.") These procedures are to be followed by all employees and independent contractors where applicable.
Procedures	The Company has a formal policy information security privacy policy and information security program that is appropriate with the size and complexity, the nature and scope of the Company's activities, and the sensitivity of the information in the Company's possession. As part of this program, The Company maintains a Privacy Policy Notice (see attached) that is posted on The Company's website and provided to customers and consumers for each order processed. Additional information about The Company's privacy and information security program is available to consumers and customers upon request. The Company policies associated with the privacy and information security program are given to all employees and the employees must acknowledge in writing that they have read and understand such policies. It is the responsibility of the Office Administrator to help ensure The Company has received all employee acknowledgements. The Company makes an annual assessment of the standards and requirements affiliated with The Company's information security program, including those set out in this policy and procedure document. This

assessment is conducted by our underwriter, Old Republic National Title Insurance Company, and a formal report on compliance is issued to The Company management.

Physical Security of NPI

The Company utilizes Nexus/Lexus and Experian as the information provider for background and credit checks. The Company individuals who have access to NPI is restricted to authorized principals and employees who have undergone a formal background check and credit report process which identified no irregularities. This practice is limited to employee's potential employees only.

The use of removable media devices, including but not limited to external hard drives, compact discs, magnetic tapes and USB/flash drives is prohibited unless The Company Manager has authorized such use. Removable media is kept in a secure area and accounted for via The Company Manager when not in use. There are currently no laptops used by The Company.

Other standard procedures for security of NPI include closing paper files other than the one currently being worked on, stowing files away when away from workspace, and locking desks and file cabinets at the end of the day. Hardcopy NPI that is transmitted outside The Company is done so using only secured envelopes and/or locked document bags.

Network Security of NPI

At the direction of The Company Manager, The Company's designated Network Administrator grants appropriate access to The Company's various computer technology applications. The Company's file server(s) or main central processing unit is located in-house in a secured server room. The Company's computer network utilizes up-to-date anti-virus, anti-spyware and data encryption software applications. The Network Administrator, Terry Anderson, President of Secure Data Services, is responsible for such software maintenance.

Access to The Company's information technology computers and network is secured by the Office Administrator and has access to the unique passwords. The Company utilizes a computer application that prompts employees to change passwords every 30 days. All The Company's computers run a "screen timeout" application causing automatic system sign off when the system detects no activity for a period of three (3) minutes.

Disposal of NPI

The Company has defined and communicated to employees the types of data/information that falls into the NPI category. A large, secure shredding bin provided by J. M. Stevens Shredding Services can be found in the office and documents are shredded on the premises monthly. When disposing of computers and portable storage devices, The Company's uses our Network Administrator to use a software application to erase/wipe clean the computers and/or devices.

	Disaster Management Plan for NPI The Company has a documented disaster management plan to help ensure adequate back-up, recovery and business continuation procedures. The plan also includes required procedures for notification and response to security incidents and breaches. The disaster management plan is reviewed on an annual basis by The Company's Office Administrator and President and updated as appropriate. **Security Practices of Independent Service Providers** If independent service providers for The Company receive NPI from The Company, The Company shares this policy document with the service provider and/or conducts appropriate due diligence of the NPI security measures of the service provider before transmitting any NPI data. Service providers are aware they must notify The Company regarding NPI security breaches of NPI data that has been transmitted. If security breaches occur, proper notification is provided to consumers and law enforcement in accordance with The Company's privacy and information security program and disaster management plan.

Contact Officer	*Marc L. Shapiro, P.A., President*
Date Approved	*January 8, 2015*
Date of Commencement	*January 8, 2015*
Amendment Dates	*August 11, 2015; August 31, 2015; September 3, 2015; September 17, 2015*
Date for Next Review	*January, 2016*
Related References and Links	• *The Privacy Policy Notice is located in the Office Administrator's office.* • *The Information Security Privacy Policy Plan is located in the Office Administrator's office.* • *The Disaster Management Plan is located in the Office Administrator's office.* • *The Insurance Policies are located in the Office Administrator's office.* • *The Network Administrator is Secure Data Services, Terry Anderson, President and be contacted by: tanderson@securedsi.com*