Thomas C. Santoro PA
Attorney at Law

Policies and Procedures

Privacy and Information Security

Purpose	Document a privacy and information security program (policies and procedures) to help ensure **Thomas C. Santoro PA** maintains written protocols for the protection of data and Non-public Personal Information (NPI).
Scope	These policies and procedures are for all of **Thomas C. Santoro PA** (hereafter referred to as “The Company”) locations including all satellite offices. These procedures are to be followed by all employees and independent contractors where applicable.
Procedures	The Company has a formal privacy 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 manager to help ensure The Company has received all employee acknowledgements. The Company makes an assessment annually 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 Thomas C. Santoro and a formal report on compliance is issued to The Company management.

Physical Security of NPI

The Company utilizes FDLE 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.

Removable media devices, including but not limited to external hard drives, compact discs, magnetic tapes and USB/flash drives are issued by the Company with the approval of Thomas C. Santoro. The use of removable media devices is prohibited unless Thomas C. Santoro has authorized such use. Removable media is kept in a secure area and accounted for via Thomas C. Santoro when not in use.

Other standard procedures for security of NPI include closing paper files other than the one currently being worked on, stow files away when away from workspace and lock 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 Thomas C. Santoro, 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 housed in the account manager’s office. The Company’s computer network utilizes up-to-date anti-virus, anti-spyware and data encryption software applications. The Network Administrator is responsible for such software maintenance.

Access to The Company’s information technology computers and network is secured by individual and unique passwords. The Company utilizes a computer application that prompts employees to change passwords in regular frequency 90 days. All The Company’s computers no mater, desktop or laptop run a “screen timeout” application causing automatic system sign off when the system detects no activity for a period of 2 hours.

Disposal of NPI

The Company has defined and communicated to employees the types of data/information that falls into the NPI category. Any NPI data is disposed of accordingly. Paper records by shredding. Small shredders are available throughout the office. Large, secure shredding bins provided by Cintas can also be found in the office. When disposing of computers and portable storage devices, The Company uses a software application to erase/wipe clean the device.

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 Company also maintains insurance coverage, commercial property insurance, and liability coverage for such circumstances. The disaster management plan is reviewed on an annual basis by the office manager 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	*Thomas C. Santoro*
Date Approved	*September 1990*
Date of Commencement	*September 1990*
Amendment Dates	*January 2014* *January 2015* *January 2016* *January 2017* *January 2018* *January 2019*
Date for Next Review	*January 2020*
Related References and Links	*Internal Company Policies:* • *Privacy and information security program policies and where they are kept*