Data Security Policy

Security Statement
Veritas Title Partners, L.P. has taken measures to guard against unauthorized or unlawful processing of personal data and against accidental loss, destruction or damage.
This includes:

- Adopting an information security policy (this document is our policy)
- Taking steps to control physical security (projects and staff records are all kept in a locked filing cabinet or locked offices)
- Putting in place controls on access to information (***password protection on files and server access***)
- Establishing a business continuity/disaster recovery plan (including, at a minimum taking regular back-ups of its computer data files and this is stored away from the office at a safe location)
- Training all staff on security systems and procedures
- Detecting and investigating breaches of security should they occur

Basic Principles

1. Personal data is to be collected only for the purpose specified in the Data Security Policy.
2. Data collected is to be relevant but not excessive for the purposes required.
    - On an annual basis, title insurance request and open order forms and any other forms that we use are reviewed to confirm that we are not asking for irrelevant information
3. Data is not to be kept for longer than is necessary for the purposes collected, including complying with applicable laws. Within 30 days of closing:
    - Files are scanned into our secure server and paper copies are shredded, or
    - Files are moved to locked files in a secure location in our office
4. We protect the data with appropriate technical and organizational measures to minimize the risk of unauthorized or unlawful processing and against accidental loss or destruction or damage to personal data.
    - Servers are stored in locked facilities with access limited to IT and Management personnel only.
    - Remote access to files is available only to personnel with background checks.
5. Data is not removed from the office, except when contained on/within appropriately secured data transmission methods.
    - Paper files are never removed from the office except as needed for a remote closing and only handled by the Escrow Officer handling said closing.
    - Remote access is provided to our server for Escrow Officers and Management personnel only.
    - When access is provided, the following security measures are in place: It is a condition of remote access to the office network by staff that their home computers provided by our company and managed by our IT only. They also have anti-virus software installed which is regularly updated with the latest virus definitions by our IT staff.

6. Access to data whether current or archived is provided to those individuals who, in the course of performing their responsibilities and functions, must use the specified data.
   Access is limited to the following job positions: Escrow personnel with current background checks only
7. All data on the network is protected by Computex - Iron Port anti-virus software that runs on servers and workstations, and is updated automatically with on-line downloads from the Simantec or Macafee website. This includes alerts whenever a virus is detected.
8. Any viral infection that is not immediately dealt with by Akisha Networks is notified to the Chief Financial Officer, Michael A. Knudsen.
9. All user data is backed up automatically on a daily basis, using an appropriately secure system for fast indexing and data restoration.
10. A full server backup takes place daily.
11. Daily backups are securely stored in a room remote from the server room.
12. A separate business continuity plan is established.