Lighthouse Title Best Practices 3 – Information Security Statement

Lighthouse Title Group has taken measures to guard against unauthorized or unlawful processing of personal data and against accidental loss, destruction or damage.

This Includes:

- Adopted an information security policy (this document is our policy).
- Established steps to control physical security and “clean desk” policies.
- Established controls on access to information (password protection on files and server access).
- Implemented a business continuity/disaster recovery plan (including, at a minimum taking regular backups of its computer data files and this is stored away from the office at a safe location).
- Train staff members on privacy laws, rules and regulations thru Real Estate Data Shield.
- Established protocol for detecting and investigating breaches of security should they occur.

Principles:

1. Personal data is to be collected only for the purpose specified and is only able to be accessed by authorized personnel.
2. Data collected is to be relevant but not excessive for the purposes required.
3. Data is not to be kept for longer than necessary for the purposes collected. Within 10 days of closing, files are scanned into our secure server and paper copies are shredded by a secured shredding service.
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.
    a. Servers are stored in locked facilities
    b. Facilities that house our servers are only accessible through multiple layers of security: proxy card/standard key (building access), building alarm system and standard key to the server room.
    c. Remote access to files is only available with the proper credentials
    d. The computers are disconnected from the internet and turned off, during non-business hours.
    e. Data is accessible only with proper authority.
    f. Firewalls (multiple levels), Intrusion Detection Systems, and Anti-Virus/Spam protection solutions are in place to protect data.
5. Data is not removed from the office, except when contained within appropriately secured data transmission methods.
    a. Paper files are not removed from the office except as needed for a remote closing by authorized personnel.
    b. Remote access is only provided to our server for employees.

6. Access to data whether current or archived is provided to those individuals who, in the course of performing their responsibilities and functions, must be a member of that specific security group.
7. All data on the network is protected by McAfee VirusScan Enterprise anti-virus / anti-spam software that runs on servers and workstations, which is updated automatically with virus definitions as released by the manufacturer, Network Associates / McAfee. Administrators will be notified if any computer has been infected with a virus.
8. All viral infections are dealt with immediately and the end-user that is infected is logged off until the infected profile is fixed.
9. All user data is backed up to disk automatically on a daily basis.
10. A full server backup to disk takes place when a server is brought into production, followed by incremental backups to disk on a daily basis.
11. All backups are automatically replicated to a remote facility at least 32 miles away from the primary data center.
12. A business continuity plan, in case of catastrophic loss, is regularly reviewed and updated.