Accounting Security

RECOMMENDED PROCEDURES:

- ✓ Restrict access to Non-public Personal Information to authorized employees.
- ✓ Prohibit or control the use of removable media.
- ✓ Use pragmatic measures when transmitting sensitive information. Secure methods are highly recommended, but may be impractical or cost-prohibitive depending on circumstances.
- ✓ Take reasonable steps to protect any network, including the restriction of access by authorized individuals only.
- ✓ Develop clear & concise guidelines for the appropriate collection and transmission of Non-public Personal Information.
- ✓ Implement a method of secure disposal of Non-public Personal Information. Any consideration should account for physical & digital media.
- ✓ Establish a disaster management plan.
- ✓ Implement a continuous program of training to help ensure compliance with Company's guidelines and protocols.
- ✓ Establish accountability criteria for all vendors/service providers, such as proof of insurance, bonding, etc.
- ✓ Regular auditing and oversight of personnel and procedures to help ensure compliance with Company's procedures and protocols.
- ✓ Adopt and maintain a process to report and address the misuse/abuse of personal, non-public information.
- ✓ Companies should provide disclosure to consumers and customers as to their privacy requirements.

Information provided by Escrow Institute - Carlsbad California January 2014

Distributed By Dick Jonilonis & Associates

619 460-8925 dickj@pmsoftwaresolutions.net

DJ&A
DICK JONILONIS & ASSOCIATES