Note: Because of numerous requests by PIA members, former Executive Vice President Elsie Reamy wrote this document as a guide only. It has not received regulatory approval, but it may be of assistance to you.

One Agency's Administrative Safeguards

Training

All of our employees are made fully aware of the agency's security policy. They are trained to comply with all security procedures including the correct use of information processing in order to minimize any security risk. Each employee is fully aware that failure to comply with any security procedure may result in a suspension and possible termination of employment.

Risk Assessment

Our agency management periodically reviews its security controls to ensure that polices and controls respond to changes in business requirements and priorities that may present new threats and vulnerabilities to our agency.

Information Clarification

Information is classified to indicate the degree of protection necessary to protect information commensurate with the risk and to allow for appropriate protection, control, and accountability.

Media Handling Security

We have implemented procedures to protect documents, computer media, and system documentation from damage, theft, and unauthorized access. Those procedures are defined in other sections of this document.

Disposal of Data and Documents Containing Customer Information

It is our policy to retain customer information for as long as a policy stays in force and for three (3) calendar years after a policy cancels. (*This is Virginia's requirement; if you keep information longer than that, put your policy here.)* When a file reaches the end of the previously described lifecycle, all documents contained in that file that hold any non-public information are shredded prior to disposal.

Disposal of computer Equipment

Prior to disposing of any computers, we ensure that the hard drives are completely erased by qualified professionals.

E-Mail Content Review

To ensure that electronic mail content is used for legitimate business purposes, an agency principal or delegate *(list your person here)* may examine the content of electronic mail and other electronic communications without prior notice.

Internet/Intranet Usage

Internet and intranet must be confined to the normal tasks required for the operation of this business. Employees are forbidden to access sites that may put this agency at risk of embarrassment. Examples of forbidden sites include any that relate to pornography, racism, gambling, and criminal activities. Only approved applications may be downloaded or installed from the intranet or the Internet as needed or required by companies with whom we do business.

Disaster Recovery Planning

Most companies with which we do business are Internet based and the electronic files are managed and maintained by those companies. It is important to note that we also keep paper *(or electronic, if that is the case)* files in support of the insurance company files.

One Agency's Technical Safeguards

User Identifications (IDs) and Passwords

The following systems are in place to protect our electronic files from being accessed by unauthorized individuals: (1) User IDs and passwords are restricted to owner access and use only. Only agency owners or those they delegate will provide initial user IDs and passwords. When passwords are subsequently reset, they are recorded in a restricted log, kept in a locked location, and accessible only to the agency owners or their delegates. Employees are required to notify the agency owner or their delegates when a password is changed so the security log is correct at all times. Employees are asked to choose passwords that are resistant to attack, maintain secrecy of the passwords, and report password security violations to the agency owner or those delegated. (2) Passwords must comply with size, letter, and numerical sequence as required for each application where a password is needed. (3) When an employee no longer works for the agency, his or her access to the system is denied.

Antivirus Application

Every computer is protected by Norton Anti-Virus Professional Edition, a product of Symantec, Inc. *(If you use a different antivirus system, list it instead.)* This system provides for automatic screening every night and automatically checks for program updates. These updates should assure we always have the best possible antivirus protection available. It is our policy to be certain that no second-hand software is used on any computer unless it is first approved by the agency owner or those delegated and scanned for viruses. Our system is further protected from all unauthorized access via the Internet or intranet by a highly effective firewall system called Black Ice. *(If you use a different firewall, list it instead.)* This system allows only specific systems and protocols to communicate throughout network perimeter.

Remote Location Access

Except in an extreme emergency, only the agency owner or those delegated have access to our remote (third) location. In such an emergency, one other person *(list name or position)* has authorization to use that unit.

Unattended Workstations and Terminals

When a terminal is left unattended, written customer information is removed from top of desk; screens automatically lock and can be re-opened by only the principal user of that terminal. Employees are expected to lock their systems when they expect to be away from their terminal for long periods of time. Examples include lunch hours, out-of-office projects, and the end of the day. Screen savers are enabled after a maximum of 15 minutes of keyboard/mouse inactivity.

Vendor Support and Modems

Our online access is provided by Roadrunner. *(List your online access provider here.)* All vendor troubleshooting support communications require link encryptions.

Banner Messages

Any person attempting to gain access will receive a banner message that provides the following warning: "This system is for authorized use only. Any use of this system without approved authority is subject to prosecution. All activities on this system are monitored and recorded by system personnel. In the course of monitoring this system or in the course of system maintenance, the activities of authorized users may be monitored. Anyone using this system expressly consents to monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide evidence for use by law enforcement or other authorized agencies."

Physical and Environmental Security Policy

♦Because of the nature of the information in these files, all financial products subject to National Association of Security Dealers (NASD) scrutiny (variable life and annuities and mutual funds) are stored separately from all other files in file cabinets that are locked at the end of every business day.

♦All computer hardware is plugged into high performance surge protection units.

♦Fire extinguishers are present and easily located in each office.

♦Office entrances are secured with deadbolts.

♦Money is kept in a safe, and checks are kept in a locked cabinet.

♦Access to computers is difficult because of the use of passwords to unlock them and the number of user Ids and passwords needed to access applications.

End of Elsie's Suggested Security Policy