Information Security Program

Licensed insurance entities are required to develop a comprehensive written customer information security program pursuant to Sections 501, 505(b) and 507 of the federal Gramm-Leach-Bliley Act and corresponding sections of state regulation (when applicable).

We believe that the administrative, physical and technical safeguards outlined below are appropriate to the size and complexity of our operation and the nature and scope of our activities. This program is designed to describe how we:

1. ensure the security and confidentiality of customer information;
2. protect against any anticipated threats or hazards to the security or integrity of the information; and
3. protect against any unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

Administrative safeguards: procedures

Staff training and awareness

1 We have designated an individual or committee to oversee our information security program.

2 We have reviewed with our employees (existing and new) relevant information security policies and procedures that apply to them as set forth in this information security program.

3 We have developed an action plan should a security breach occur.

4 Employees are instructed to report suspected security breaches.

5 We have a policy requiring employees to verify the identity of persons requesting customer information.

6 Employees are instructed to keep customer information confidential when outside of the professional setting (such as where conversations could be overheard).

7 Access to confidential information is limited to those employees who have a business reason for seeing it.

Service provider/other provider(s) oversight

1 The agency exercises due diligence in selecting its service providers (such as checking references prior to retaining).

2 The agency requires all service providers to execute a service provider agreement.

3 The agency exercises due diligence in selecting its other providers (such as checking references prior to retaining).

4 The agency reviews security procedures with its service providers.

Disposal of information

1 Documents containing customer information are shredded or otherwise destroyed before disposal.

2 Electronic files or media containing customer/consumer information are destroyed or 'wiped' prior to disposal.

Maintenance and review of program

1 We monitor, evaluate and adjust our information security program, as appropriate.

Physical safeguards: security of agency office premises

General office security

1 All access points to the premises are adequately secured by locks or locking devices.

2 Our internal policy outlines which individuals have keys to the premises.

3 We have a policy against the duplication of keys.

4 We have a policy to secure keys immediately from terminated employees.

5 Our premises is sufficiently lit at night.

Visitor policy and reception area

1 Visitors are greeted immediately upon entry to the premises.

Access to Agency Files & Hardware

1 Records are stored in protected or controlled areas.
2 Filing cabinets are locked after working hours.
3 Our internal policy requires employees not to leave consumer/customer information open to public view.
4 Employees are required to follow security procedures if they are permitted to remove files from the premises.
5 Employees are instructed to lock their desks after working hours.
6 The agency's server is located in a protected or controlled area.
7 Computer monitors are turned away from visitors.

Technical safeguards: systems security

Anti-virus software

1 Anti-virus protection software is installed on the network.
2 Anti-virus protection software is installed on all office computers.
3 Office computers are scanned for viruses on a regular basis.
4 Our policy prohibits our employees from disabling anti-virus software.
5 We have activated the automatic update feature for virus definitions.
6 We have activated the automatic update feature for the antivirus program.
7 We have a procedure in place to deal with a virus infection.

Anti-spyware software

1 Anti-spyware software is installed on all office computers.
2 Office computers and servers are scanned with anti-spyware on a regular basis.
3 Our policy prohibits employees from disabling anti-spyware software.
4 The automatic update features for anti-spyware definitions have been activated.
5 We have activated the automatic update feature for the anti-spyware program.

Firewalls

1 Our office is equipped with a network firewall.
2 Our office computers are equipped with individual firewalls.
3 Our Internet Service Provider (ISP) uses filters to help prevent access to unauthorized users.
4 Our workstations' file-sharing capability has been shut off or disabled.
5 We have a procedure in place to update the firewall software.
6 We have a policy in place to test the integrity of our firewall and other intrusion protection systems.

Network and program password protection

1 Our internal policy requires passwords that are difficult to guess.
2 Employees' passwords must be between six and eight characters and include at least one lower-case letter, one upper -case letter, and one number.
3 Employees are required to change passwords regularly (at least every 90 days).
4 When employees change their password, our internal policy prohibits them from reusing the same password within a 12-month period.
5 Access will be denied if the correct password is not entered after a certain number of attempts.
6 Employees are instructed not to share their passwords.
7 Employees are instructed not to leave their passwords in a visible location.

8 We have a procedure for removing individuals from system access immediately upon termination.

Data backup

1 The agency backs up network data on external media (tapes, CD's and/or DVD's) at least weekly.

2 Back-ups are stored safely in a secure offsite location.

3 Backups are tested at least quarterly. These tests should be done as a restore from the backup tapes to a separate location (test environment), not just a validation that the backup ran successfully.

Laptops

1 Our internal policy prohibits staff/guests from using personal laptops and hardware on our computers and network without permission.

2 Access control software is installed on all employee laptops that contain agency information or that have access to agency systems.

3 Laptops are patched with the latest operating system patches.

4 Laptops are equipped with up-to-date firewall and virus protection software.

Email policy

1 We have a policy relative to the monitoring of employee emails.

2 Employees are instructed not to open and to delete emails from unknown sources or with unusual captions.

3 Our internal policy prohibits the transmission of confidential information via email without the use of encryption software.

System user instructions

1 Employees are instructed to close out of all network-based applications when away from their desks.

2 Employees are instructed to log off their password-protected internet-based applications when away from their desks.

3 Employees are instructed to close their web browser when they are away from their desks or when it is not in use.

4 Our internal policy prohibits employees from downloading or installing software on the agency?s computer system without prior approval.

5 Employees are instructed not to download files from unknown sources.

6 Our internal policy prohibits our employees from using instant-messaging software.

User monitoring

1 Our agency monitors network traffic to detect any unusual activities.

2 Our agency actively manages the logs produced by the security components available on our system (firewall, wireless router, proxy server, fax server, etc.).