THE ASSOCIATION ADVANTAGE

Information Security Plan

effective March 1, 2010

The Association Advantage LLC
591 North Avenue, Suite 3-2 Wakefield, MA 01880-1617
781/245-6485 Fax 781/245-6487
Solutions@TheAssociationAdvantage.net www.TheAssociationAdvantage.net

THE ASSOCIATION ADVANTAGE

I. OBJECTIVE:
   a. Our objective, in the development and implementation of this written information security plan, is to create effective administrative, technical and physical safeguards in order to protect our company and our clients and their members' non-public, personal information. The plan evaluates our electronic and physical methods of accessing, collecting, storing, using, transmitting, protecting, and disposing of our company and our clients' non-public, personal information.
   b. Hereafter, all of the policies and procedures refer to both our company and our client associations and members' non-public, personal information

II. PURPOSES:
   a. Ensure the security and confidentiality of information.
   b. Protect against any anticipated threats or hazards to the security or integrity of this information.
   c. Protect against unauthorized access to or use of information that could result in substantial harm or inconvenience.

III. ACTION PLANS:
   a. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of information or information systems.
   b. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of information.
   c. Evaluate the sufficiency of existing policies, procedures, information systems, and other safeguards in place to control risks.

IV. ACTION STEPS:
   a. Appoint a specific person or persons within the organization to be responsible for:
      i. Initial implementation of plan
      ii. Training of employees
      iii. Regular testing of the controls and safeguards established by the plan
      iv. Evaluating the ability of prospective service providers to maintain appropriate information security practices, ensuring that such providers are required to comply with this information security plan, and monitoring such providers for compliance herewith.
      v. Periodically evaluating and adjusting the plan, as necessary, in light of relevant changes in technology, sensitivity of customer information, reasonably foreseeable internal or external threats to customer information, changes to information systems.
   b. Conduct an annual meeting for all employees on the elements of this information security plan, the contents of privacy policies, and any other requirements of federal or state privacy laws. All persons following the guidelines of this information security plan are required to sign a contract to uphold the policies within this information security plan.
   c. Determine reasonably foreseeable **internal** threats that could result in unauthorized disclosure, misuse, alteration, or destruction of company or client information or information systems, assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of information, and evaluate the sufficiency of existing policies, procedures, information systems, and other safeguards in place to control risks.

Action Steps continued

Internal Threat	Risk Level	Response
Intentional or inadvertent misuse of company or client information by current employees	Low	**1.** Dissemination and annual review of privacy laws and individual client privacy policies. **2.** Employment agreements amended to require compliance with privacy policies and to prohibit any nonconforming use of information during or after employment. **3.** Employees are encouraged to report any suspicious or unauthorized use of information. **4.** Periodic review to ensure these safeguards are implemented uniformly.
Intentional or inadvertent misuse of information by former employees subsequent to their employment	Low	**1.** Require return of all information in the former employee's possession (i.e., policies requiring return of all organization property), including laptop computers and other devices in which records may be stored, files, records, work papers, etc. **2.** Eliminate access to information (i.e., policies requiring surrender of keys, ID or access codes or badges, business cards; disable remote electronic access; invalidate voicemail, e-mail, internet, passwords, etc.), and maintain a highly secured master list of all lock combinations, passwords, and keys. **3.** Change passwords for current employees periodically. **4.** Amend employment agreements during employment to require compliance with privacy policies and to prohibit any nonconforming use of information during or after employment. **5.** Send "pre-emptive" notices to clients when the organization has reason to believe a departed employee may attempt to wrongfully use information, informing them that the employee has left the company. **6.** Encourage employees to report any suspicious or unauthorized use of information. **7.** Periodic review to ensure these safeguards are implemented uniformly.
Inadvertent disclosure of information to the general public, contracted specialists or guests in the office	Low	**1.** Prohibit employees from keeping open files on their desks when leaving for the day or a substantial period of time. **2.** Require all files and other records containing company and client records to be secured at day's end. **3.** Use a software program that requires each employee to enter a unique log-in ID to access computer records and to re-log in when the computer is inactive for more than a few minutes. **4.** Change passwords periodically. **5.** Restrict guests to one entrance point. **6.** Use shredding machines on unused photocopies or other records being discarded before depositing in trash or recycling containers. **7.** Ensure secure destruction of obsolete equipment, including computer hardware and software items. **8.** Encourage employees to report any suspicious or unauthorized use of information. **9.** Periodic review to ensure these safeguards are implemented uniformly. **10.** Require all sensitive records to be maintained in locked desks or filing cabinets when the office is closed.

Action Steps continued

d. Determine reasonably foreseeable **external** threats that could result in unauthorized disclosure, misuse, alteration, or destruction of information or information systems, assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of information, and evaluate the sufficiency of existing policies, procedures, information systems, and other safeguards in place to control risks.

External Threat	Risk Level	Response
Inappropriate access to, or acquisition of information by third parties	Low	**1.** Install firewalls for access to internet sites. Include privacy policy on Internet sites. **2.** Require secure authentication for internet and/or intranet and extranet users. **3.** Require encryption and authentication for all infrared, radio, or other wireless links. **4.** Train employees to protect and secure laptops, handheld computers, or other devices and media used outside the office that contain sensitive information. **5.** Install virus-checking software that continually monitors all files, downloads, floppy disks, CDs, USB sticks, all incoming and outgoing e-mail messages. **6.** Establish uniform procedures for installation of updated software. **7.** Establish systems and procedures for secure back-up, storage and retrieval of computerized and paper records. **8.** Establish procedures to ensure external points of entry to the office are closed, locked and inaccessible to unauthorized persons when the office is closed. **9.** Physically lock or otherwise secure the computers, and areas in which sensitive paper records are stored. **10.** Use shredding machines on unused photocopies or other records being discarded before depositing in trash or recycling containers. **11.** Ensure secure destruction of obsolete equipment, including computer hardware and software systems. **12.** Encourage employees to report any suspicious or unauthorized use of information. **13.** Periodic review to ensure these safeguards are implemented uniformly.
Inappropriate use of information by third parties	Low	**1.** Evaluate the ability of all prospective third-party service providers to maintain appropriate information security practices. **2.** Provide all third-party service providers to whom contractual access to premises or records has been granted (including, but not limited to, insurance companies being solicited for new or renewal policies, mailing houses, custodial or plant services, equipment or service vendors, affiliates, non-affiliated joint marketing partners,…) with a copy of the Privacy Policies. **3.** Require all such third-parties-**by written contract**-to adhere to the Privacy Policies, agree to make no use of any nonpublic personal information that would be prohibited thereby, or otherwise by law or contract, and agree to hold harmless and indemnify the company for any inappropriate use of non-public personal information.

Inappropriate use of information by third parties continued		**4.** Require all such third-parties-**by written contract**-to return all information and property at the completion or termination, for whatever reason, of the agreement between the company and the third-party. **5.** Prohibit access to information (i.e., policies requiring surrender of keys, ID or access codes or badges, disabling remote electronic access; invalidating voicemail, e-mail, internet, passwords, etc…, if applicable) to all such third-parties upon completion or termination, for whatever reason, of the agreement between the company and the third-party. **6.** Change passwords for current employees periodically. **7.** Send "pre-emptive" notices to clients when the company has reason to believe a terminated third-party service provider may attempt to wrongfully use information, informing them that the agreement with the company is no longer in effect. **8.** Encourage employees to report any suspicious or unauthorized use of information. **9.** Periodic review to ensure these safeguards are implemented uniformly.

THE ASSOCIATION ADVANTAGE

Addendum A - Document Retention and Destruction Policy & Procedures

The Association Advantage LLC shall retain records for the period of their immediate or current use, unless longer retention is necessary for historical reference or to comply with contractual or legal requirements. Records and documents outlined in this policy include paper, electronic files (including emails) and voice mail records regardless of where the document is stored, including network servers, desktop or laptop computers and handheld computers and other wireless devices with text messaging capabilities. Any employee of The Association Advantage LLC, or any other person who is in possession of records belonging to The Association Advantage LLC who is uncertain as to what records to retain or destroy, when to do so, or how to destroy them, may seek assistance from The Association Advantage LLC's Document Retention Policy (DRP) manager who is Sherri Oken, CAE, Executive Director.

In accordance with 18 U.S.C. §1519 and the Sarbanes Oxley Act, The Association Advantage LLC shall not knowingly destroy a document with the intent to obstruct or influence an investigation or proper administration of any matter within the jurisdiction of any department, agency of the United States or in relation to or contemplation of such matter or case. If an official investigation is under way or even suspected, document purging must stop in order to avoid criminal obstruction.

The retention periods described herein are guidelines. There are circumstances under which a record or document may have to be maintained longer than the guidelines. This will be a decision made by the Document Retention Policy Manager.

In order to eliminate accidental or innocent destruction, THE ASSOCIATION ADVANTAGE LLC has the following document retention policy:

Type of Document	**Minimum Requirement**
Accounts payable ledgers and schedules	7 years
Audit reports	Permanently
Bank Reconciliations	2 years
Bank statements	3 years
Checks (for important payments and purchases)	Permanently
Contracts, mortgages, notes and leases (expired)	7 years
Contracts (still in effect)	Permanently
Correspondence (general)	2 years
Correspondence (legal and important matters)	Permanently
Correspondence (with customers and vendors)	2 years
Deeds, mortgages, and bills of sale	Permanently
Depreciation Schedules	Permanently
Duplicate deposit slips	2 years
Employment applications	3 years
Expense Analyses/expense distribution schedules	7 years
Year End Financial Statements	Permanently
Insurance Policies (expired)	3 years
Insurance records, current accident reports, claims, policies, etc.	Permanently
Internal audit reports	3 years
Inventories of products, materials, and supplies	7 years
Invoices (to customers, from vendors)	7 years
Minute books, bylaws and charter	Permanently
Patents and related Papers	Permanently

Payroll records and summaries	7 years
Personnel files (terminated employees)	7 years
Retirement and pension records	Permanently
Tax returns and worksheets	Permanently
Timesheets	7 years
Trademark registrations and copyrights	Permanently
Withholding tax statements	7 years

**Source of information serving as background guidance in determining THE ASSOCIATION ADVANTAGE LLC's organization's document retention policy. *©2004 National Council of Nonprofit Associations, www.ncna.org*

THE ASSOCIATION ADVANTAGE

Addendum B - Security Policies and Procedures

General Principles

- The Association Advantage LLC, as an independent contractor, will with discretion and confidentiality, perform the contracted administrative, management and consulting services in consideration of agreed upon annual payments.
- We will protect the privacy of our clients and members, and respect the information disclosure policies set forth by their boards of directors.
- We will safeguard our client's records and data to the best of our ability.

Computer Technology and Security

We evaluate and upgrade hardware on a regular basis, as well as utilize systems to safeguard our clients' data. All data is protected by firewalls and virus protection software.

Data Backup

- Our networked system operates off a server with redundant hard drives and an external tape back-up that automatically backs up our full system daily.
- Weekly, we create additional back up media for databases and financial records:
  Flash drive/memory stick media is encrypted for additional security.
- Software but not records or data is maintained on our lap top computer.

Firewalls

- Lynksys Network Translation (NAT) Firewall: Model WRT 54G
- Windows Firewall

AntiVirus Protection

- Norton AntiVirus Software
- Symantec Endpoint Protection – also anti-spamware

Insurance

- *The Association Advantage* carries general liability insurance in the amount of $2,000,000. Our policy includes $10,000 Employee Dishonesty coverage.
- If check-writing privileges are granted by an association, the appropriate staff person will be bonded.