



Agency Information Security Plan
Development Materials

As of September 13, 2010

Disclaimer

ACT is providing this prototype agency information security plan solely as a tool to assist agencies and brokers in creating a plan appropriate and customized for their particular firm. This sample is not a substitute for agencies and brokers independently evaluating any business, legal or other issues, and is not a recommendation that a particular course of action be adopted. State **security breach notification and privacy laws, coupled with insurance laws and regulations, impose varying requirements on agencies and brokers. Therefore, it is extremely important for agencies and brokers to carefully review applicable laws and regulations in all jurisdictions where they do business in structuring their specific security plans. We have worked off the laws of Massachusetts in formulating this prototype plan, because Massachusetts imposes some of the most specific requirements. If specific advice is required or desired, the services of an appropriate, competent professional should be sought.**

Note: Bracketed comments ([**Note:**]) are used throughout the prototype plan to provide guidance to agencies in formulating their plans. They should not be included in any final plan, but instead should be converted into customized provisions in the agency plan, where appropriate.

[Sample Insurance Agency, Inc.]

INFORMATION SECURITY PLAN

DEFINITIONS

Please carefully review the definition of these terms, because they are used frequently in this plan:

“Plan” refers to the Information Security Plan.

“Agency” refers to [insert agency name here].

“Clients” refers to the Agency’s clients, former & prospective clients.

“Encrypted” refers to the use of a program to put computer data into a coded format that cannot be read by unauthorized users.

“Passwords” refers to a string of characters that, when possible, is at least 8 characters long and contains at least three of the following: upper case letter, lower case letter, a number, a special character (%, &, #, etc.).

“Private Information” refers to non-public personal, proprietary and confidential information, of Clients, the Agency and/or Agency employees.

“Systems” refers to all agency computers, networks, copiers, scanners, FAX machines, voice mail/phone systems, and other storage devices (e.g. back-up tapes, USB and other portable drives, CDs, etc.) where Agency Private Information might be found (whether maintained on Agency equipment/servers or on equipment/servers managed by third parties or employees, wherever located).

SCOPE & OBJECTIVE

This Plan for Agency is intended to create effective administrative, technical, electronic and physical protections to safeguard the personal information of the Agency’s Clients and employees, the Agency’s proprietary and confidential information, the physical security of our premises, and the integrity of our electronic systems so that they are best positioned to function smoothly without interruption.

This Plan sets forth the Agency’s procedures for electronic and physical methods of accessing, collecting, storing, using, transmitting, destroying, and protecting Private Information of Clients, the Agency and/or Agency employees and also the use of the Agency’s Systems by Agency employees and any authorized third parties, as deemed appropriate and/or required by applicable laws and regulations.

In formulating and implementing this Plan, we have:

- (1) identified reasonably foreseeable internal and external risks to Agency’s security, confidentiality and/or integrity of electronic, paper or other records containing Private Information;
- (2) assessed the likelihood and potential danger of these threats, taking into consideration the sensitivity of the Private Information;
- (3) evaluated the sufficiency of existing Agency policies, procedures, and other safeguards in place to minimize those risks;

(4) designed and implemented an approach that puts safeguards in place to minimize those risks, consistent with the requirements of applicable laws/regulations; and

(5) included regular monitoring of the effectiveness of those safeguards.

All security measures contained in this Plan shall be reviewed and re-evaluated annually or when there is a change in applicable laws or regulations or in the business activities of Agency. The Agency reserves the right to modify this Plan at any time, with or without prior notice.

[Note: Federal and state privacy laws and regulations typically provide that the particular administrative, technical, electronic and physical safeguards a business incorporates into its security program be appropriate to the size and complexity of the business and the nature and scope of its activities. Thus, it is important for agencies to customize this prototype plan to the nature and scope of its business activities.]

[Note: It is critical for Agency to actually implement all of the elements it includes in its Information Security Plan (whether it means incorporating new technologies, procedures, workflows, training, monitoring, audits, etc.), because it is likely the agency's plan will be referenced by regulators or in future lawsuits should a security breach occur. It is also important for agencies to carefully review the privacy statements that they provide to consumers and that they safeguard the confidentiality of all of the information they commit to protect in these statements.]

[Note: Just as agencies are encouraged to review and re-evaluate their security plans on an annual basis, this prototype plan should be considered a living document and will need to be updated regularly as new security risks become known or reasonably expected.]

EMPLOYEE RESPONSIBILITY

It shall be the responsibility of each Agency employee to carefully read, understand and adhere to this Plan. Each employee with access to Private Information shall receive training as necessary on this Plan and confirm in writing that he or she understands the requirements and will adhere to it as a continuing condition of his or her employment. Failure to adhere to the requirements of this Plan shall subject the employee to disciplinary action by Agency, up to and including termination.

[Note: This plan is directed toward "employees" throughout. If the Agency uses independent contractors as well as employees, the Agency will need to broaden the plan to cover this group, such as by substituting "Agency Users" for "employees" wherever the term appears and defining "Agency Users" to include all categories of the Agency's workers.]

OWNERSHIP OF AGENCY INFORMATION

The Agency regards all information contained, sent or received on the Agency's Systems and/or Agency equipment (e.g., Agency computers and mobile electronic devices, email, text and instant messaging systems, social networks and message boards, whether maintained on Agency equipment/servers or on equipment/servers managed by others) as well as information contained in, sent or received by Agency employees about the Agency or relating to its business on non-Agency equipment, as the property of the Agency, and the Agency reserves the right to access,

review, use and disclose any such information at any time, with or without notice to employee, in Agency's sole discretion. Employees have no right to or expectation of privacy with respect to any such information (except for the Private Information relating specifically to them), and shall acquire no ownership or control rights over such information.

[Note: Any monitoring of conversations and communications using Agency's equipment (e.g., phones, computers, mobile devices, etc.) or involving Agency business must be conducted in accordance with applicable laws/regulations, and should be expressly described in writing to Agency's employees, such as in a policy manual. The lack of an expectation of privacy in the work place also can be covered in other Agency policies, such as a policy covering use of electronic communications and equipment. This would also cover other things like the Agency policy on restricting downloading on Agency equipment of third party software not provided by Agency, limiting use of Agency equipment for personal communications, etc.]

INFORMATION SECURITY COORDINATOR

The Agency has designated [VP of Information Technology (or other title designated for this responsibility)] as the "Information Security Coordinator" to oversee implementation of this Plan.

The Information Security Coordinator will be responsible for:

1. Initial implementation of this Plan;
2. Training existing and new employees;
3. Appropriate testing and evaluation of this Plan's safeguards;
4. Evaluating the ability of service providers to comply with this Plan and applicable laws/regulations;
5. Reviewing the security measures in this Plan annually or when there is a change in applicable laws or regulations or in business activities of Agency; and
6. Conducting training as necessary for all Agency employees with access to Private Information.

[Note: The Information Security Coordinator can be designated by position in the Agency's Plan, rather than by name, so staff changes do not automatically necessitate changes to the Plan.]

SPECIAL PROTECTION FOR PRIVATE INFORMATION

Private Information is to be accorded the highest level of confidentiality by the Agency and employees.

Examples of Private Information include, but are not limited to

1. First name and last name, or first initial and last name, **and** any one or more of the following:
2. Social Security number;
3. driver's license number, passport number, or state-issued identification card number;
4. financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password; and/or
5. personal or protected health information.

The information listed in 2-5 above, even if it is not connected with a name, should each be treated as Private Information because of the potential for identity to be stolen from possession of just the numbers or information.

[Note: Agency should carefully review **security** breach notification and privacy laws, as well as insurance laws/regulations, in all states where it does business, as well as in the states in which individuals on which Agency holds Private Information reside, to make sure this definition of Private Information encompasses all of those laws/regulations. The privacy laws typically require that the business keep confidential the information that an individual gives it. The Private Information identified above are the kinds of **information** elements that typically trigger state security breach notification laws, which require notification of the affected individuals, regulators, etc., as well as other statutory requirements, in the event of a breach of Private Information. [Click here](#) for a list of the state security breach notification laws, as published by the National Conference of State Legislatures.

[Note on HIPAA: Agency should also carefully review the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules to assure compliance with any requirements that are applicable, such as regarding the treatment of Protected Health Information (PHI). For further information on HIPAA and its privacy and security rules, see <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html>.]

WHERE PRIVATE INFORMATION IS STORED

The Agency and its employees recognize that the Agency possesses Private Information in the following places, whether in the Agency's premises or off site, and whether created or maintained by Agency or third parties on behalf of Agency:

- hard copy and electronic files on Clients and employees, located at desks, in file drawers, storage areas and on the Agency's Systems;
- personnel files, Form I-9s, benefits information, payroll information, and direct deposit information for employees wherever located, including but not limited to hard copies at desks, in file drawers and other storage areas, and in electronic form on the Agency's Systems;
- off-site back-ups, in any form; and
- third-party vendors entrusted with Private Information from the Agency.

This Plan is intended to protect Private Information possessed by the Agency from unauthorized access, dissemination and/or use.

Private Information may not be disseminated, communicated or stored on or through any social media websites or services, at any time or for any reason.

[Note: The Agency should carefully identify every place in which it maintains Private Information to make sure it is identified and thus properly handled and protected, and so it is stored and accessible only to those with a need to access it to do their jobs.

The Agency should also determine whether it truly needs to keep that Private Information in all the places it exists, or at all, and if not, the unneeded information should be properly destroyed (e.g., paper documents shredded, and electronic materials destroyed or securely deleted (including electronic back-ups)) in accordance with the Agency's Plan and any applicable laws.]

INTERNAL RISKS TO PRIVATE INFORMATION & AGENCY SECURITY

To combat internal risks to the security, confidentiality and/or integrity of records containing Private Information, the following measures will be taken:

1. Agency employees will access Private Information only for appropriate business purposes, as necessary, within their job duties.
2. The Agency will encrypt and password-protect Private Information in its Systems to the extent reasonably practical, as determined by Agency management.
3. The Agency will retain only the last four digits of credit card numbers and will not retain bank routing numbers, personal bank account numbers and checks, and all credit- and banking-related information not retained will be destroyed in accordance with applicable law and Agency-designated business practices.
4. Paper files containing Private Information will be locked when not in use so Private Information is not accessible to others, and electronic files containing Private Information will not be left accessible to others, such as on computers or portable storage devices accessible (e.g., computer screens must be locked when an employee using such files leaves his or her computer, even briefly). Paper and electronic files must not be removed from the Agency premises or accessed remotely unless specific authorization has been provided in advance, and **then, the security of that Private Information must be maintained.**
5. Employees are expected to log off or lock their computers when they **leave them unattended (such as when on breaks, at lunch, in a meeting or out of the office).** The Agency will implement controls to terminate computer sessions and/or **lock computers** after a predetermined time of inactivity (e.g., 30 minutes).

Agency computers will require a user ID and password and Agency mobile devices should require a password (and be encrypted, if reasonably feasible). Employee log-ins and passwords should be appropriately strong (with the minimum number of characters and other elements required by the Agency's Systems). The Agency will remind all employees of the requirement to change their computer passwords every 90 days, and employees will not share their password(s) with any other employees and will secure these passwords in a locked drawer or password-protected file. Electronic access to Private Information will be blocked after multiple unsuccessful attempts to log-in.

Employees should keep mobile electronic communications devices (such as PDAs, BlackBerries, smart phones, etc.) with access to Private Information in their possession or in a secured location at all times, and Employees will not share passwords or other access information with others.

Employees will not put any Agency data on thumb drives, laptops or other portable media, drives and devices unless authorized by the Agency. If so authorized, the thumb drives, laptops or other portable media, drives and devices must be password-protected and encrypted, and the portable mobile electronic communications devices and laptops must be password-protected and encrypted.

[Note: Agency should implement technology that permits remote wiping of all data from lost mobile devices, if available.]

[Note: If an unencrypted mobile device that contains Private Information is lost, it may trigger a reporting requirement under some state security breach notification laws, even if it is password-protected, so it is important to have a reporting process so the Information Security Coordinator or other responsible person can assure the Agency adheres to applicable laws.]

6. Employees will adhere to the Agency document retention schedule and requirements. When it is appropriate to destroy Agency records, paper and electronic records containing Private Information must be destroyed in a manner in which Private Information cannot be read or reconstructed. Unless otherwise directed by the Information Security Coordinator, a commercial shredding company will be used to destroy paper documents. When computers, digital copiers, scanners and/or printers with electronic storage capacity, or portable electronic devices and media are discarded, such disposal should be coordinated with the Information Security Coordinator, and care needs to be taken to ensure that the hard drives or other storage media are destroyed in a manner that all data becomes unreadable.
7. Employees will not be given access to carrier website passwords where those carriers can be accessed through the Agency's Real Time tools. Instead, these passwords will be managed and kept up-to-date by the Information Security Coordinator (or Agency Administrator). The Information Security Coordinator is

responsible for terminating all of the employee's IDs and passwords to the Agency's Systems, as well as carrier and other third party websites, and invalidating the employee's access to Agency intranet and Agency-sponsored social media, immediately upon the employee's ceasing to work for the Agency or when directed by Agency management.

[Note: Some agencies may want to implement an alternative provision where carrier passwords are maintained by individual employees. Such a provision might provide:

"Employees are required to maintain carrier and other passwords in a password-protected and encrypted electronic folder that is also accessible by the Information Security Coordinator. The Information Security Coordinator shall be notified immediately of any employee ceasing to work for the Agency, so that he or she can take immediate action to deactivate all passwords to which the former employee had access."]

8. Employees that no longer work for the Agency must: (1) return to Agency all Agency information (including, but not limited to, any Private Information) in any form, whether stored on computers, laptops, portable devices, electronic media, or in files, records, work papers, etc.; (2) return all keys, IDs, access codes and/or badges; and (3) not access non-public Agency information (including, but not limited to, any Private Information).
9. In accordance with the Agency's human resources manual, access by the former employee to Agency email and voice mail accounts can be immediately disabled and access transferred to other Agency staff to assure a continuity of work, and inactivated when determined appropriate by Agency.
10. Employees are required to report all actual or potential unauthorized access to, use of or disclosure of Private Information to the Information Security Coordinator.

EXTERNAL RISKS TO PRIVATE INFORMATION & AGENCY SECURITY

In addition to the measures taken to combat internal risks, the following measures will be taken to minimize external risks to the security, confidentiality and/or integrity of records containing Private Information:

1. Visitors to the Agency will be escorted within the office and will not have access to Agency computers or property that may contain Private Information. Guests' wireless access should be fire-walled off from the Agency's Systems.
2. The Agency will maintain security measures so that its wireless networks cannot be accessed remotely by the public.
3. During non-office hours, the Agency will be locked and have a central station-reporting security system activated.

4. Cleaning crews and other vendors providing maintenance and repair services to the Agency's premises will be appropriately screened, and no Private Information will be left out or accessible to such workers.
5. Servers and other equipment at the Agency's premises containing Private Information will be maintained in a secure location.

[Note: It is recommended that agencies maintain their servers in a locked computer room when possible.]

6. Employees should not open any email attachment, link, or application where the employee does not reasonably believe the information expected to be accessed is from a trustworthy source. Employees will not use Agency equipment to access any application or software not approved by the Agency.
7. The Agency will employ an email filter (hardware, software, or third-party provided) that works to restrict and eliminate viruses, spyware and other malware before getting to Agency desktop and portable computers.
8. The Agency will maintain up-to-date network and firewall protection and operating system security patches on its Systems, servers and desktop and laptop computers, as well as other security measures deemed appropriate. The Agency will maintain security software, which includes malware protection with up-to-date patches and virus definitions, on its Systems and its servers, desktop and laptop computers, and all mobile devices, which is updated as frequently as possible, but at least daily.

[Note: Agency should set procedures that define the time frames when new software versions relating to each element of its Systems must be implemented.]

9. All back-ups will be password-protected **and encrypted and** kept in a secured location off site.
10. Agency employees should use care in communications (e.g., outgoing email and attachments) to ensure: first, that the Private Information needs to be sent by email and, if so, that it is transmitted using secure email in accordance with Agency policy.

[Note: ACT strongly recommends the use of TLS email encryption where the carrier or client can accept it. This results in the most friendly workflow for both the sender and the receiver. Otherwise the email can be sent using a proprietary email solution (if the carrier or other party will accept it) or password-protected file (such as a password-protected PDF), where the password is delivered separately from the email containing the file and consists of information that only the end user will know. For more information on TLS email encryption, see the "Security & Privacy" section at www.independentagent.com/act.

Also note that password protecting a file may not be sufficient to avoid triggering a **security** breach under the state security breach notification laws if sent to the wrong place or recipient.]

[Note: If the Agency uses a voice over Internet phone (VoIP) system, then the Agency should ascertain the level of security protections built into the transmissions as they pass over the Internet to determine if any special measures need be taken or special directions need to be given to Agency staff.]

11. The Agency will create a secure SSL tunnel between its website and the consumer before allowing the consumer to enter any Private Information or to enter a password.
12. When an employee accesses Agency Systems and/or Private Information from a remote location, the Agency's secure SSL connection must be used (such as Virtual Private Network, GoToMyPC, LogMeIn). Private Information transmitted across public networks or wirelessly should always be encrypted.
13. Employees should not access Agency Systems or Private Information using non-Agency equipment (e.g., a home computer) unless authorized by the Agency and provided with appropriate firewalls and virus protection, and done through the Agency's secure SSL connection. Employees will not store any Private Information on any non-Agency equipment.
14. The Agency may monitor its Systems and equipment for unauthorized use, including but not limited to implementing hardware, software and/or procedural mechanisms to record and report activity for the Systems and equipment, without further notice to employees.
15. The Agency will exercise due diligence in making sure third-party vendors that are provided Private Information have the requisite security controls and written plan in place, provide the Agency a written commitment to safeguard and store Private Information with at least the same level of security controls as the Agency maintains (as outlined in this Plan), and advise the Agency as to any actual, suspected or potential breaches of Private Information.

[Note: These vendor commitments need to track the requirements of applicable state security breach notification and other privacy laws and regulations, as well as the Agency's Plan.]

IF A BREACH OF PRIVATE INFORMATION OCCURS OR IS SUSPECTED

A security breach occurs when there is an unauthorized acquisition, dissemination, use or loss of Private Information. Each employee shall be responsible for notifying the Information Security Coordinator whenever he or she learns that there has been or *may* have been a security breach that may have compromised Private Information or other Agency information about Clients, employees or Agency business.

The Agency will take the following actions in the event of a security breach:

[Note on Red Flags Rule: The Agency should determine whether it must comply with the Red Flags Rule, designed to fight identity theft by requiring “creditors” with certain kinds of accounts to implement compliance programs to detect and prevent identity theft (the enforcement of which has been delayed through December 31, 2010). Each Agency operates differently and thus needs to assess the definitions under the Rule carefully to determine if it must comply. Information on who must comply with the Rule, as currently written, and implementing a written compliance program can be found in the Big “I” summary of the Rule in a memo titled, “Overview of the Fair Credit Reporting Act, the Fair and Accurate Credit Transactions Act, and the Drivers Privacy Protection Act,” starting on page 10 at letter G. This memo is available to Big “I” members who log in to www.independentagent.com, click on “Legal Advocacy” and select “Memoranda and FAQs.” A “how to” guide for businesses, a video explaining the Rule, and a “do-it-yourself” template for low-risk businesses are all available on the FTC’s website [here](#) (and see particularly the FAQs).]

[Note on Additional Requirements of HIPAA: If the agency is a “Business Associate” that handles “protected health information” (“PHI”) for a “Covered Entity,” as defined by the HIPAA Privacy Rule, then it will have to conform this plan to the additional security requirements that are mandated by the HIPAA Security Rule, as well as comply with a whole host of other HIPAA requirements, which are beyond the scope of this Plan. See the HHS website for a great summary of the requirements of the HIPAA Security Rule-- <http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html>]

* * * * *

For additional resources on agency security and privacy, please go to www.iiaba.net/act and click on the “Security & Privacy” link in the gray shaded area on the left of the page.

Acknowledgements

ACT wishes to thank the members of its Agency Security Best Practices and Security Issues Work Groups, as well as IIABA’s Office of General Counsel, for their work in developing and providing input into this prototype plan. ACT gives special thanks to the Massachusetts Association of Insurance Agents for permitting us to use the Information Security Plan it had developed for its members as a starting point in the creation of this prototype plan.