

**ASCINSURE SPECIALTY RISK**  
**PRIVACY/SECURITY PLAN**  
**July 15, 2010**

**OBJECTIVE**

This Security Plan (the "Plan") is intended to create effective administrative, technical and physical safeguards for the protection of personal information of employees who are residents of the Commonwealth of Pennsylvania. The Plan sets forth the Agency's procedure for evaluating electronic and physical methods of accessing, collecting, storing, using, transmitting and protecting personal information of residents of the United States of America. (the "Resident").

For purposes of this Plan, "personal information" means:

A Resident's first name and last name, or first initial and last name, in combination with any one or more of the following that relate to such resident:

- (a) Social Security number;
- (b) Driver's license number or government, state-issued identification card number
- (c) Financial account number, or check, credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account, or;
- (d) Individually identifiable information, in electronic or physical form, regarding the individual's medical history, medical treatment, or diagnosis by a health care professional.

The Agency recognizes that, in particular, it possesses the personal information of Residents in the following places:

- hard copy customer and prospective customer files located in file cabinets or desk drawers
- Electronic customer files or driver database located on the agency management system (AMS360), agency in-house compute servers, CD-ROM, USB drives, E-Mail Server and/or individual employee PC computer hard drives/laptops/USBdrives/CD-ROM.
- Personnel files and benefits information for agency employees located in locked file cabinets in the locked office of the VP of Administration.
- Form I-9s for agency employees located in locked file cabinets in the locked office of the VP of Administration.
- Payroll information for agency employees, including direct deposit information located in locked file cabinets in the locked office of the VP of Administration.

This Plan is intended to protect this information from unauthorized access and/or use.

## **SCOPE**

In formulating and implementing the Plan, we have (1) identified reasonably foreseeable internal and external risks to the security, confidentiality and/or integrity of any electronic, paper or other records containing personal information; (2) assessed the likelihood and potential danger of these threats, taking into consideration the sensitivity of the personal information; (3) evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to minimize those risks, (4) designed and implemented a plan that puts safeguards in place to minimize those risks, consistent with the requirements of various State regulations, and (5) plan to regularly monitor the effectiveness of those safeguards.

## **DATA SECURITY COORDINATOR**

The Agency has designated Susan Mason as the Security Coordinator to implement, supervise and maintain the Plan.

The Data Security Coordinator will be responsible for:

1. Initial implementation of the Plan;
2. Training employees;
3. Regular testing of the Plan's safeguards;
4. Evaluating the ability of service providers to comply with the law;
5. Reviewing the scope of the security measures in the Plan at least annually, or whenever there is a material change in business practices affecting the Plan;
6. Conducting an annual training session for all agency employees with access to personal information.

## **INTERNAL RISKS TO PERSONAL INFORMATION**

To combat internal risks to the security, confidentiality and/or integrity of records containing personal information, including any and all customer files, the following measures will be taken:

1. Agency employees should access customer files only for legitimate business purposes.
2. Only Martin O'Brien, President and Kathy Wieland, VP of Administration shall have access to employee personnel files, payroll information and employees' benefit information.
3. Files containing personal information should be maintained under lock and key when not in use. If an employee needs to transport records containing personal information outside of the agency premises, reasonable steps should be taken to maintain the security of the information.
4. When it is appropriate to destroy agency records, paper and electronic records containing personal information must be destroyed in a manner in which personal information cannot be read or reconstructed. Each employee will empty their "shredding" box daily.
5. Employees must be aware of their surroundings at all times, and notify the Security Coordinator of any breach in security immediately.
6. Agency computers shall require a user ID and password. Current employees' computer user-IDs and passwords will be changed periodically. Electronic access to personal information shall be blocked after multiple unsuccessful attempts to log-in.

7. Each Password must consist of eight (8) characters and include at least one of the following: Upper case letter(s), Lower case letter(s), Number(s), Symbol(s).
8. Employees are to keep all Passwords in a safe and secured plan. No Passwords will be displayed on the computer terminals, left in the open on their desks etc. Passwords will be provided to Kathy Wieland, VP of Administration, Brian Thomas, IT Consultant, and the Employee's direct supervisor for emergency access in the event the Employee is unavailable.
9. Employees MUST log-off the Agency Network upon leaving the office. The workstations may remain on but at the log in screen. All Employee computers (workstations) will be set to automatically log off the Employee after being idle for five minutes. All Employee computers must be logged off when stepping away from their workstation.
10. Terminated employees must: (1) return all records containing personal information, in any form (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.), (2) return all keys, IDs, access codes and/or badges, (3) be prohibited from accessing personal information and (4) the terminated employee's access to e-mail, voicemail, agency intranet and passwords will be invalidated.
11. Electronic access to personal information shall be restricted to active users and active user accounts only.
12. Employees are encouraged to report any suspicious or unauthorized use of customer information.
13. All security measures contained in this Plan shall be reviewed and reevaluated annually, or whenever there is a material change in the business.
14. Employees with access to personal information will be trained on this Plan.
15. Agency employees who violate this Plan may be subject to discipline up to and including termination.

The Agency should ensure that vendors who are provided personal information have their own compliant written security plan.

### **EXTERNAL RISKS TO PERSONAL INFORMATION**

To minimize external risks to the security, integrity of records containing personal information, including any and all customer files, the following measures will be taken:

1. All Employees will strictly adhere to the "All-Hazard Plan" as provided by Allegheny General Hospital, building owner of Four Allegheny Center, Pittsburgh, Pa. This Plan is posted on the Agency's Intranet.
2. The Agency's "Disaster Recovery Plan" is posted on the Agency's Intranet and outlines the procedures to follow during a disaster and/or evacuation.
3. Visitors to the agency shall check-in with the Building's security desk at the entrance of the building and sign-in accordingly.
4. Visitors to the agency shall not have access to records containing personal information.
5. Visitors to the agency shall be restricted to the reception area and/or the conferences rooms situated at the front of the office, unless otherwise approved by the Security Coordinator.

6. All Visitors to the agency should make an appointment with the appropriate Agency employee as feasibly possible. Unknown or Unauthorized Persons/Visitors to the Agency must be reported to the Building security desk immediately.
7. Use of the restrooms located outside of the Agency office is restricted to the Agency employees and their visitors.
8. Entrance to the Agency's office is restricted to the front door. The front door will be locked during the hours of 5:00 pm to 7:30 am the following day. The emergency door located in the rear of the office will be kept externally locked at all times.
9. All employees of the Agency are required to maintain the highest level of security when handling customer or Agency proprietary information. No information will be released to the public or outside sources unless the information is needed to perform the duties of their position.
10. The Agency maintains up-to-date firewall protection and operating system security patches.
11. The Agency maintains up-to-date versions of security software, which includes mal-ware protection with up-to-date patches and virus definitions.
12. To the extent technically feasible, personal information stored on laptops or other portable devices is encrypted.
13. To the extent technically feasible, personal information transmitted across public networks or wirelessly is encrypted.
14. Computer systems are monitored for unauthorized use. Brian Thomas, IT consultant for the Agency, will monitor computer systems for any breach of security or unauthorized use and report it to the Security Coordinator immediately.
15. Secure user protocols are in place, including: (1) protocols for control of user IDs and other identifiers, (2) a secure method of assigning and selecting passwords, and (3) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect.
16. Employee log-ins and passwords are not vendor supplied default log-ins and passwords.

### **IN THE EVENT A BREACH OF PERSONAL INFORMATION OCCURS**

A security breach occurs when there is an unauthorized acquisition or use of personal information of one or more Residents. The following measures will be taken by the Agency in the event of a security breach which creates a risk of identity theft to Residents:

1. The Agency will notify the Office of Consumer Affairs and Business Regulations (OCABR), the Attorney General's Office of the Commonwealth of Pennsylvania, and the Attorney General's Office of the State of residency of the Resident. This notice shall include the nature of the breach, the number of Residents affected by the breach and all the steps the agency has taken to rectify the incident and to prevent any further breaches from occurring.
2. The Agency shall also notify the employee(s) or customer(s) affected by the breach. That notice shall include information concerning each Resident's right to obtain a police report and how to request a security freeze on their consumer report, but shall not include information regarding the nature of the breach and the number of Residents affected.

**Federal Trade Commission (FTC) Red Flags Rules  
Identity Theft Prevention Program  
Effective April 1, 2010**

**Purpose:**

Compliance with FTC regulations (the Red Flags Rules) applicable to certain financial institutions which require covered financial institutions to implement a program to detect, prevent and mitigate instances of identity theft in accordance of the Fair and Accurate Credit Transactions (FACT) Act of 2003.

**Procedure:**

Any Employee who becomes aware of any transaction, conduct or circumstances considered Red Flags under FTC guidelines as they now exist or may hereafter be modified including:

- Receipt of alerts, notifications or warnings from a consumer reporting agency involving a **transaction account** or a **covered account**
- Receipt of suspicious documents involving a **transaction account** or a **covered account**
- Receipt of suspicious personally identifying information , such as a suspicious address, involving a **transaction account** or
- Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with **covered accounts**

shall make the Security Coordinator aware of such circumstances, in writing, as soon as is reasonably practicable but not later than 24 hours following the time at which such Employee became aware of such alerts, documents, suspicious personally identifying information or notices. The Security Coordinator will promptly conduct an investigation and take appropriate action including but not limited to the filing of a report or reports with applicable authorities and notifying the customer, customers or holders of the affected **covered accounts**.

**Program Management:**

This program is under the direct management of the Agency Management Team and will be updated with notice from time to time as may be required to comply with regulatory changes and/or operational changes within the organization.

**Definitions:**

- A **Transaction Account** is a deposit or other account from which the owner makes payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.
- A **Covered Account** is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. **Covered Accounts** include credit card accounts, mortgage loans, automobile loans, margin accounts, utility accounts checking accounts and savings accounts. A **Covered Account** is also an account for which there is a foreseeable risk of identity theft – for example small business or sole proprietorship accounts.