PILOT
CATASTROPHE SERVICES, INC.

Personal Identifiable Information & **Privacy** Policy
Last Modified: February 23, 2017

It is Pilot's policy to comply with all state and federal laws in regards to Personal Identifiable Information (PII) of Pilot's employees, clients and its clients' customers. Pilot's philosophy is to safeguard PII in its electronic possession (ePII) and to ensure the confidentiality of this information. ePII is information which is computer based, and is used or stored on digital media and equipment, including but not limited to computers, laptops, disks, memory sticks, PDA's, servers, networks, dial-modems, E-Mail or websites. The scope of this policy is intended to be comprehensive and includes company requirements for the security and protection of such information throughout the company and its approved vendors both on and off work premises.

The objectives of this policy are to: incorporate, develop and implement this comprehensive written information security program (WISP); to create effective administrative, technical and physical safeguards for the protection of PII; and to comply with all applicable government regulations and obligations. The policy sets forth our procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII.

PII may reside in hard copy or electronic records; both forms of PII fall within the scope of this policy. Pilot will only collect PII or ePII that is required to pursue its business operations and to comply with government reporting and disclosure requirements. PII or ePII collected by the company includes but is not limited to:

- **Identifiable contact information**: first or last names, addresses, telephone numbers, e-mail addresses, other identifiers that could cause contact.
- **Demographic Information**: date of birth, number of dependents, family composition, age or gender of children, height, weight, race, religion, occupation, education, products owned, political party affiliation, veteran's status.
- **Financial Information**: bank account routing number and account number, credit/debit card numbers, bank or investment accounts, payment history, assets, income level, credit worthiness, spending habits.
- **Online navigation or tracking information**: online cookies, personal internet address, personal web site, any online information to identify the customer.
- **Government issued identification numbers**: Social Security Number, Federal Tax Identification Number, driver's license number.
- **Credit Card information**: corporate or individually held credit or debit transaction card numbers (including PIN or access numbers) maintained in organizational or approved vendor records.

All employees are required to follow and use the guidelines set forth in this policy and HR 700 Computer Technology Usage to ensure that the necessary steps to safe guard ePII and PII are taken.

Data Security Coordinator:

Pilot has designated Pilot's Human Resources Department Manager to implement, supervise and maintain this policy and WISP. This designated employee (Data Security Coordinator) will be responsible for or coordinating the implementation of the following:

1. Implementation of the WISP including all provisions outlined in this policy

2. Ensure training of all employees
3. Regular testing of the policy's safeguards
4. Evaluating the ability of any of our third party service providers to implement and maintain appropriate security measures for the PII to which we have permitted them access, and requiring such third party service providers by contract to implement and maintain appropriate security measures
5. Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing PII
6. Conducting periodic training session for all owners, managers and employees who have access to PII on the elements of the WISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with our requirements for ensuring the protection of PII.

Vendors: Approved individual(s) or companies who are recipients of organizational PII and from which the Technology Services Department (TSD) has received certification of their data protection practices conformance with the requirements of this policy. Vendors include all external providers of services to the company and include proposed vendors. No PII information can be transmitted to any vendor in any method unless the vendor has been approved for the receipt of such information.

PII Retention: Pilot understands the importance of minimizing the amount of PII data it maintains and retains such PII only as long as necessary. A joint task force comprising members from the Legal, Finance, TSD, and Human Resources departments maintains organizational record retention procedures, which dictate the length of data retention and data destruction methods for both hard copy and electronic records in accordance with HR 185 Record Retention and Destruction Policy.

PII Training: All new hires entering the company who may have access to PII are provided with introductory training regarding the provisions of this policy, a copy of this policy and implementing procedures for the department to which they are assigned. Employees in positions with regular ongoing access to PII or those transferred into such positions are provided with training reinforcing this policy and procedures for the maintenance of PII data and shall receive periodic training regarding the security and protection of PII data and company proprietary data

PII Audit(s): Pilot conducts audits of PII information maintained by the company in conjunction with fiscal year closing activities to ensure that this policy remains strictly enforced and to ascertain the necessity for the continued retention of PII information. Where the need no longer exists, PII information will be destroyed in accordance with protocols for destruction of such records and logs maintained for the dates of destruction. The audits are conducted by Finance, TSD, Operations and Human Resources departments under the auspices of the Legal department.

Data Breaches/Notification: Databases or data sets that include PII may be breached inadvertently or through wrongful intrusion. Upon becoming aware of a data breach, the company will notify all affected customer or individuals whose PII data may have been compromised, and the notice will be accompanied by a description of action being taken to

reconcile any damage as a result of the data breach. Notices will be provided as expeditiously as possible and in no event be later than the commencement of the payroll period after which the breach was discovered.

If an employee becomes aware of a material breach in maintaining the confidentiality of customer information, the employee should report the incident to Pilot legal department at legal@pilotcat.com . The legal department has the responsibility to investigate the incident, and take appropriate action and notify all required entities. Please be aware that a standard of reasonableness will apply in these circumstances. The Legal department will handle breach notifications(s) to all governmental agencies to whom such notice must be provided in accordance with time frames specified under these laws.

Data Access: Pilot maintains multiple computer systems where PII data may reside; thus, user access to such IT systems is the responsibility of the TSD department. The TSD department has created internal controls for such systems to establish legitimate access for users of data, and access shall be limited to those approved by TSD. Any change in vendor status or the termination of an employee or independent contractor with access will immediately result in the termination of the user's access to all systems where the PII may reside.

Data Transmission and Transportation:

1. Company Premises Access to PII: The Operations, Finance, Human Resources and TSD departments have defined responsibilities for on-site access of data that may include access to PII; TSD has the oversight responsibility for all electronic records and data access capabilities. Operations, Finance and Human Resources have the operational responsibility for designating initial access and termination of access for individual users within their organizations and providing timely notice to TSD.

2. Vendors: Pilot may share data with vendors who have a business need to have PII data. Where such inter-company sharing of data is required, the TSD department is responsible for creating and maintaining data encryption and protection standards to safeguard all PII data that resides in the databases provided to vendors.

3. Portable Storage Devices: Pilot reserves the right to restrict PII data it maintains in the workplace. In the course of doing business, PII data may also be downloaded to laptops or other computing storage devices to facilitate company business. To protect such data, the company may also require that any such devices be given appropriate PII security.

4. Off-Site Access to PII: Pilot understands that employees may need to access PII while off site or on business travel, and access to such data shall be permitted, subject to the provision that the data to be accessed is minimized to the degree possible to meet business needs and that such data shall use all necessary measure to ensure PII data protection.

Regulatory Requirements: It is the policy of the company to comply with any international, federal or state statute and reporting regulations. If any provision of this policy conflicts with a statutory requirement of international, federal or state law governing PII, the policy provision(s) that conflict shall be superseded.

Confirmation of Confidentiality: All company employees must maintain the confidentiality of PII as well as company proprietary data to which they may have access and understand that that such PII is to be restricted to only those with a business need to know. No employee is authorized to release a customer PII or ePII without prior written authorization or what is

required by law, nor shall he or she move any media containing such information without management approval.

Daily Operational Protocol:

This section of our policy outlines our daily efforts to minimize security risks to any computer system that processes or stores PII, ensures that physical files containing PII are reasonably secured and develops daily employee practices designed to minimize access and security risks to PII of our clients and/or customers and employees.

The Daily Operational Protocol shall be reviewed and modified as deemed necessary at a meeting of the Data Security Coordinator and personnel responsible and/or authorized for the security of PII. Any modifications to the Daily Operational Protocol shall be published in an updated version of the policy. At the time of publication, a copy of the WISP shall be made available to all current employees and to new hires.

1. Recordkeeping Protocol:

a. We will only collect PII that is necessary to accomplish our legitimate business transactions or to comply with any and all federal and state and local laws.

b. Any PII stored shall be disposed of when no longer needed for business purposes or required by law for storage. Disposal methods must be consistent with those prescribed by the policy. Any paper files containing PII shall be stored securely under lock and key.

c. Only department heads and the Data Security Coordinator will be assigned keys to secure file areas and only those individuals are allowed access to the paper files. Individual files may be assigned to employees on an as-needed basis by the department supervisor.

d. All employees are prohibited from keeping unsecured paper files containing PII in their work area when they are not present (e.g. lunch breaks). At the end of the day, all files containing PII are to be returned to the secure file area.

e. Paper or electronically stored records containing PII shall be disposed of in a manner as follows:

(a) Paper documents containing PII shall be either redacted, burned, pulverized or shredded so that PII cannot practicably be read or reconstructed;

(b) Electronic media and other non-paper media containing PII shall be destroyed or erased so that PII cannot practicably be read or reconstructed.

f. Media containing PII or ePII must be stored in a physically secure location with access limited to those with business need-to-know. If sent, it must be done so by secured courier or other method that can be accurately tracked.

2. Where practical, electronic records containing PII shall not be sent or transmitted electronically to any portable device, or sent or transported electronically to any computer, portable or not, without being encrypted, unless there is no reasonable risk of unauthorized access to the PII Access Control Protocol:

a. All our computers shall restrict user access to those employees having an authorized and unique log-in ID assigned by the Data Security Coordinator.

b. After 5 unsuccessful log-in attempts by any user ID, that user ID will be blocked from accessing any computer or file stored on any computer until access privileges are reestablished by the Data Security Coordinator or his/her designee.

c. Access to electronically stored records containing PII shall be electronically limited to those employees having an authorized and unique login ID assigned by the Technology Services Department.

d. Where practical, all visitors who are expected to access areas other than common space or are granted access to office space containing PII should be required to sign-in with a Photo ID at a designated reception area where they will be assigned a visitor's ID or guest badge unless escorted at all times. Visitors are required to wear said visitor ID in a plainly visible location on their body, unless escorted at all times. Where practical, all visitors are restricted from areas where files containing PII are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing PII are stored.

e. Cleaning personnel (or others on site after normal business hours and not also authorized to have access to PII) are not to have access to areas where files containing PII are stored.

f. All company computers with an internet connections or any computer that stores or processes PII must have a reasonably up-to-date version of software providing virus, anti-spyware and anti-malware protection installed and active at all times.

g. An inventory of all company computers and handhelds authorized for PII storage will be maintained by the Technology Services Department.

3. Third Party Service Provider Protocol:

a. Any service provider or individual that receives, stores, maintains, processes, or otherwise is permitted access to any file containing PII ("Third Party Service Provider") shall be required to meet the standards of this policy as well as any and all government standards.

b. Any contract with a Third Party Service Provider shall be the responsibility of the Data Security Coordinator to obtain reasonable confirmation that any Third Party Service Provider is capable of meeting security standards of this policy and all government regulations. Any existing contracts with Third Party Service Providers shall be reviewed by the Data Security Coordinator.

Violations of PII Policies and Procedures:

Pilot views the protection of PII data to be of the utmost importance. Infractions of this policy or its procedures will result in disciplinary actions under the company's discipline policy and may include suspension or termination in the case of severe or repeat violations. PII violations and disciplinary actions are incorporated in the company's PII training to reinforce the company's continuing commitment to ensuring that this data is protected by the highest standards.