

Philadelphia Insurance Companies Information Security Policy

The Philadelphia Insurance Companies uses advanced technology and information management techniques to implement security, audit and control programs designed to ensure the security and confidentiality of consumer records and information.

In establishing its Information Security policies and procedures, Philadelphia Insurance Companies considers the following key factors in its risk assessment:

1. *Access rights to consumer and customer information*
 - Access rights to consumer and customer information are granted to authorized individuals by Company management. Rights are assigned on an as-needed basis. For example, Company Vice Presidents will have a greater amount of access to applications than would a data entry clerk. Access to all systems and files are controlled through the use of the Windows NT operating system.
2. *Access controls on consumer and customer information systems, including controls to authenticate and grant access only to authorized individuals and companies.*
 - Access to consumer and customer information is restricted to authorized individuals. All of the Company's applications are utilizing authentication technology to control access. Authorized individuals are assigned a unique username and password to use when attempting to logon to applications containing consumer and customer information. In addition, after three unsuccessful attempts the user is locked out of the system and must be reset by the system administrator.
3. *Access restrictions at locations containing consumer and customer information, such as buildings, computer facilities, and records storage facilities.*
 - Philadelphia Insurance Companies data center is located in its home office location. At this location, physical access to the building is controlled through the use of an access card system. In addition, security guards patrol the premises at all times.
 - Access to the computer facilities (data center) is controlled through the use of an access card system. Only authorized individuals (such as Information Technology personnel) are granted access to the data center.
 - Philadelphia Insurance Companies uses an outside vendor as its offsite records storage facility. Security surrounding the vendor's facility has been verified through visits to the vendor's site.
4. *Encryption of electronic consumer and customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access.*
 - Information in storage on networks or systems to which unauthorized individuals may have access is encrypted. We are currently in the process of implementing technology that will protect data in transit.
5. *Procedures to confirm that consumer and customer information system modifications are consistent with the licensee's information security program.*

- Change management procedures are closely adhered to when making modifications to systems containing consumer and customer information. These procedures ensure that access to confidential information is restricted to authorized individuals.
6. *Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to consumer and customer information.*
 - Background checks are conducted on all potential Philadelphia Insurance Companies employees, including those that may have access to consumer and customer information. Procedures for screening new hires are closely followed by the Company's Human Resources department.
 - A proper segregation of duties is accomplished through the use of detailed job descriptions. Per Company policy, job descriptions are required for each position within the organization. The job descriptions outline the general responsibilities of the employee, with a particular focus of an adequate segregation of duties.
 7. *Contract provisions and oversight mechanisms to protect the security of consumer and customer information maintained or processed by service providers.*
 - When storing backup information, the Company requires that service providers ensure the security of consumer/customer information in their possession. The Company maintains an accurate inventory of all tapes that are stored offsite with service providers.
 8. *Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into consumer and customer information systems.*
 - Philadelphia Insurance Companies' Information Technology personnel have procedures in place to monitor firewall activity on a weekly basis. When reviewing the firewall activity logs, Information Technology personnel are looking for numerous failed logon attempts and strange looking usernames. All suspicious events are investigated thoroughly.
 9. *Response programs that specify actions to be taken when unauthorized access to consumer and customer information systems is suspected or detected.*
 - Information Technology personnel are responsible for providing up to date response programs in the event that there are actual or attempted intrusions into our information systems.
 10. *Protection against destruction of consumer and customer information due to potential physical hazards, such as fire and water damage.*
 - Philadelphia Insurance Companies' data center is protected through the use of fire suppression equipment and the selection of the physical location and construction design of the data center.
 11. *Response programs to preserve the integrity and security of consumer and customer information in the event of computer or other technological failure, including, where appropriate, reconstructing lost or damaged customer information.*
 - Philadelphia Insurance Companies maintains a disaster recovery plan for the home office data center. In addition, business contingency plans are maintained for every department

throughout the organization. The disaster recovery plan is tested once per year at the facilities of our disaster recovery vendor.