

Commonwealth Automobile Reinsurers

Information Security Policy

I. Purpose

The Standards for the Protection of Personal Information of Residents of the Commonwealth, codified at 201 CMR 17.00, require that anyone who owns or licenses Personal Information about a resident of the Commonwealth of Massachusetts establish minimum standards for the safeguarding of such information. CAR is subject to this regulation and adopts this Information Security Policy in conformance therewith.

II. Administration

This Information Security Policy shall be implemented, maintained and overseen by the Data Security Coordinator, who shall be responsible for the initial implementation of the Plan, employee training (including an annual training session for all CAR employees with access to Personal Information), regular testing of the Plan's safeguards, evaluating the ability of service providers comply with this regulation, and reviewing the scope of the security measures in the Plan at least annually on or before January 1, or whenever there is a material change in business practices affecting the Plan.

III. Risk Assessment

CAR maintains Personal Information in several formats and locations, including hard copy paper and electronic documents, digital media, computer systems, laptops, and storage media devices. Department management is responsible for identifying how and where Personal Information is kept, developing policies and procedures for relating to the storage, access and transportation of records containing such information, and for educating the department's employees and monitoring their compliance with this Plan.

This Plan has been developed foremost to prevent any security system failure, and to ensure that a breach is detected in the event that one occurs. In order to protect the data from internal and external risks, CAR has implemented a number of technical, administrative and physical safeguards as described herein.

A. Administrative Safeguards

- Employees will receive education and training regarding the proper handling of Personal Information and the proper use of the computer security system. Employee training will be ongoing, and will include full and part time, as well as temporary and contract employees.

- Employee access to records containing Personal Information shall be limited to those employees with a business need to access such information.
- Employee compliance with policies and procedures will be monitored by department management. Disciplinary measures will be imposed for violations of this Security Policy.
- Terminated employees shall be prevented from accessing records containing Personal Information.

CAR will take reasonable steps to select and retain third party service providers who will have access to Personal Information owned or licensed by CAR that are capable of maintaining appropriate security measures to protect such Personal Information consistent with state and federal regulations. Additionally, after March 1, 2010, CAR will require such service providers to affirm in writing that they will implement and maintain appropriate security measures for Personal Information owned or licensed by CAR.

B. Technical Safeguards

To minimize internal and external risks to the security of Personal Information owned or licensed by CAR, the following technical safeguards are in place:

- Secure user authentication protocols
 - All users have distinct IDs and passwords. Passwords are composed of a combination of alphanumeric and special characters.
 - Data security passwords are maintained in a location and/or format that does not compromise the security of the data they protect.
 - Access is restricted to active users and active user accounts only.
 - Access to user identification shall be blocked after multiple unsuccessful attempts to authenticate to the network.
- Secure access control measures
 - Access to records and files containing Personal Information is restricted to those who need such information to perform their job duties.
 - Unique identifications plus unique passwords and not vendor-supplied default passwords, are assigned to each person with computer access and are reasonably designed to maintain the integrity of the security of the access controls.
- Personal Information data sent over the Internet or any public network is encrypted, as is all Personal Information data that is transmitted wirelessly.
- Systems shall be reasonably monitored to detect unauthorized use of or access to Personal Information.

- All Personal Information stored on laptops or other portable devices must be encrypted.
- Firewalls and operating system security patches protecting files containing Personal Information on any system that is connected to the Internet are properly configured and up-to-date.
- CAR maintains reasonably up-to-date versions of system security agent software, which includes malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

C. Physical Safeguards

- All hard copy or tangible documents containing Personal Information must be secured and physical access limited to those who need to use the information. Such documents shall be stored in locked facilities, storage areas or containers.
- Hard copy documents containing Personal Information that are no longer needed or required to be kept must be destroyed appropriately, ie. shredded.

IV. If a Breach Occurs

- For the purposes of this policy, a breach shall mean: An incident of unauthorized access to and acquisition of unencrypted or un-redacted records or data containing Personal Information where illegal use of the Personal Information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing Personal Information along with the confidential process or key constitutes a security breach. Good faith acquisition of Personal Information by an employee or agent of the business for a legitimate purpose is not a security breach; provided that the Personal Information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.
- Once a breach is learned of, the Data Security Coordinator shall conduct a mandatory post-incident review and shall document any responsive actions taken. The Coordinator shall also document any actions taken to make changes in business practices relating to the protection of Personal Information.
- Disciplinary measures will be imposed for violations of information security program rules.