

3rd Party Certification of Compliance with MA: 201 CMR 17.00

The purpose of this document is to certify the compliance of Strategic Information Resources with 201 CMR 17.00. This law protects the sensitive data of Massachusetts residents and is enforced by the Office of Consumer Affairs and Business Regulation.

1. Do you have a comprehensive, Written Information Security Program (“WISP”) applicable to all records containing personal information about a resident of the Commonwealth of Massachusetts (“PI”)?

As a credit reporting agency (“CRA”), Strategic Information Resources (“SIR”) has long been required by state and federal law to maintain written policies to protect consumer sensitive information including PI.

2. Does the WISP include administrative, technical, and physical safeguards for PI protection?

Yes

3. Have you designated one or more employees to maintain and supervise WISP implementation and performance?

Yes, we have a compliance committee who maintains and supervises all policies.

4. Have you identified the paper, electronic and other records, computing systems, and storage media, including laptops and portable devices that contain personal information?

Yes

5. Have you chosen, as an alternative, to treat all your records as if they all contained PI?

No, SIR has taken the time to identify electronic and other records, computing systems and storage media including laptops and portable devices that contain personal information.

6. Have you identified and evaluated reasonably foreseeable internal and external risks to paper and electronic records containing PI?

Yes

7. Have you evaluated the effectiveness of current safeguards?

Yes

8. Does the WISP include regular ongoing employee training, and procedures for monitoring employee compliance?

Yes

9. Does the WISP include disciplinary measures for violators?

Yes, with escalating disciplinary action to repeat offenders up to and including termination.

10. Does the WISP include policies and procedures for when and how records containing PI should be allowed to be kept, accessed or transported off your business premises?

Yes

11. Does the WISP provide for immediately blocking terminated employees' physical and electronic access to PI records (including deactivating their passwords and user names)?

Yes, employee access is terminated immediately upon release of job duties and passwords deactivated.

12. Have you taken all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such personal information in the manner provided for in 201 CMR 17.00?

Yes

13. Have you taken all reasonable steps to ensure that your third party service providers with access to personal information are applying to such personal information protective security measures at least as stringent as those required to be applied to personal information under 201 CMR 17.00?

Yes

14. Is the amount of PI that you have collected limited to the amount reasonably necessary to accomplish your legitimate business purposes, or to comply with state or federal regulations?

Yes, documents are securely stored to accomplish legitimate business purposes and to comply with state or federal regulations and then destroyed. Records that are no longer needed are destroyed.

15. Is the length of time that you are storing records containing PI limited to the time reasonably necessary to accomplish your legitimate business purpose or to comply with state or federal regulations?

Yes

16. Is access to PI records limited to those persons who have a need to know in connection with your legitimate business purpose, or in order to comply with state or federal regulations?

Yes

17. In your WISP, have you specified the manner in which physical access to PI records is to be restricted?

Yes

18. Have you stored your records and data containing PI in locked facilities, storage areas or containers?

Yes

19. Have you instituted a procedure for regularly monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of PI; and for upgrading it as necessary?

Yes, policies are reviewed by our compliance committee on an annual basis at minimum.

20. Are your security measures reviewed at least annually, or whenever there is a material change in business practices that may affect the security or integrity of PI records?

Yes

21. Do you have in place a procedure for documenting any actions taken in connection with any breach of security; and does that procedure require post-incident review of events and actions taken to improve security?

Yes, we have a written plan that covers this.

Additional Requirements for Electronic Records

22. Do you have in place secure authentication protocols that provide for:

- Control of user IDs and other identifiers? **Yes**
- A reasonably secure method of assigning/selecting passwords, or for use of unique identifier technologies (such as biometrics or token devices)? **Yes**
- Control of data security passwords such that passwords are kept in a location and/or format that does not compromise the security of the data they protect? **Yes**
- Restricting access to PI to active users and active user accounts? **Yes**
- Blocking access after multiple unsuccessful attempts to gain access? **Yes**

23. Do you have secure access control measures that restrict access, on a need-to-know basis, to PI records and files?

Yes

24. Do you assign unique identifications plus passwords (which are not vendor supplied default passwords) to each person with computer access; and are those IDs and passwords reasonably designed to maintain the security of those access controls?

Yes

25. Do you, to the extent technically feasible, encrypt all PI records and files that are transmitted across public networks, and that are to be transmitted wirelessly?

Yes

26. Do you encrypt all PI stored on laptops or other portable devices?

Yes

27. Do you have monitoring in place to alert you to the occurrence of unauthorized use of or access to PI?

Yes

28. On any system that is connected to the Internet, do you have reasonably up-to-date firewall protection for files containing PI; and operating system security patches to maintain the integrity of the PI?

Yes

29. Do you have reasonably up-to-date versions of system security agent software (including malware protection) and reasonably up-to-date security patches and virus definitions?

Yes

30. Do you have in place training for employees on the proper use of your computer security system, and the importance of PI security?

Yes