Red Flag Rule Appendix

Other Security Procedures

The following suggestions are not required by the Federal Trade Commission's "Identity Theft Red Flags Rule", however they are security procedures a utility should consider to protect consumer information and to prevent unauthorized access. Implementation of selected actions below according to the unique circumstances of utilities is a good management practice to protect personal consumer data.

1. Paper documents, files, and electronic media containing secure information will be stored in locked file cabinets. File cabinets will be stored in a locked room.

2. Only specially identified employees with a legitimate need will have keys to the room and cabinet.

3. Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.

4. Employees will not leave sensitive papers out on their desks when they are away from their workstations.

5. Employees store files when leaving their work areas

6. Employees log off their computers when leaving their work areas

7. Employees lock file cabinets when leaving their work areas

8. Employees lock file room doors when leaving their work areas

9. Access to offsite storage facilities is limited to employees with a legitimate business need.

10. Any sensitive information shipped using outside carriers or contractors will be encrypted

11. Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery of this information.

12. Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the utility.

13. No visitor will be given any entry codes or allowed unescorted access to the office.

14. Access to sensitive information will be controlled using "strong" passwords. Employees will choose passwords with a mix of letters, numbers, and characters. User names and passwords will be different. Passwords will be changed at least monthly.

15. Passwords will not be shared or posted near workstations.

16. Password-activated screen savers will be used to lock employee computers after a period of inactivity.

17. When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.

18. Sensitive consumer data will not be stored on any computer with an Internet connection

19. Sensitive information that is sent to third parties over public networks will be encrypted

20. Sensitive information that is stored on computer network or portable storage devices used by your employees will be encrypted.

21. Email transmissions within your business will be encrypted if they contain personally identifying information.

22. Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.

23. When sensitive data is received or transmitted, secure connections will be used

24. Computer passwords will be required.

25. User names and passwords will be different.

26. Passwords will be changed at least monthly.

27. Passwords will not be shared or posted near workstations.

28. Password-activated screen savers will be used to lock employee computers after a period of inactivity.

29. When installing new software, vendor-supplied default passwords are changed.

30. The use of laptops is restricted to those employees who need them to perform their jobs.

31. Laptops are stored in a secure place.

32. Laptop users will not store sensitive information on their laptops.

33. Laptops which contain sensitive data will be encrypted

34. Employees never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage.

35. If a laptop must be left in a vehicle, it is locked in a trunk.

36. The computer network will have a firewall where your network connects to the Internet.

37. Any wireless network in use is secured.

38. Maintain central log files of security-related information to monitor activity on your network.

39. Monitor incoming traffic for signs of a data breach.

40. Monitor outgoing traffic for signs of a data breach.

41. Implement a breach response plan.

42. Check references or do background checks before hiring employees who will have access to sensitive data.

43. New employees sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.

44. Access to customer's personal identify information is limited to employees with a "need to know."

45. Procedures exist for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information.

46. Implement a regular schedule of employee training.

47. Employees will be alert to attempts at phone phishing.

48. Employees are required to notify the general manager immediately if there is a potential security breach, such as a lost or stolen laptop.

49. Employees who violate security policy are subjected to discipline, up to, and including, dismissal.

50. Service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of our data.

51. Paper records will be shredded before being placed into the trash.

52. Paper shredders will be available at each desk in the office, next to the photocopier, and at the home of any employee doing work at home.

53. Any data storage media will be disposed of by shredding, punching holes in, or incineration.