QCOL, Inc. Personal Information Security Procedures

1. Paper documents, files, and electronic media containing secure information will be stored in locked file cabinets.
2. Only specially identified employees with a legitimate need will have keys to the 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. Access to offsite storage facilities is limited to employees with a legitimate business need.
9. Any sensitive information shipped using outside carriers or contractors will be encrypted.
10. Visitors who must enter areas where sensitive files are kept must be escorted by an employee.
11. No visitor will be given any entry codes or allowed unescorted access to the office.
12. 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 not be shared or posted near workstations.
13. Password-activated screen savers will be used to lock employee computers after a period of inactivity.
14. When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
15. Anti-virus and anti-spyware programs will be run on individual computers and on servers routinely.
16. When sensitive data is received or transmitted, secure connections will be used.
17. Computer passwords will be required.
18. The use of laptops is restricted to those employees who need them to perform their jobs.
19. Laptops are stored in a secure place.
20. Employees never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage.
21. If a laptop must be left in a vehicle, it should be locked in a trunk.
22. The computer network will have a firewall where your network connects to the Internet.
23. Any wireless network in use is secured.
24. Maintain central log files of security-related information to monitor activity on your network.
25. Monitor incoming traffic for signs of a data breach.
26. Monitor outgoing traffic for signs of a data breach.
27. New employees sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.
28. Access to customer's personal identify information is limited to employees with a "need to know."
29. Procedures exist for making sure that workers who leave or transfer to another part of the company no longer have access to sensitive information.
30. Employees will be alert to attempts at phone phishing and data brokers.

31. Employees are required to notify the general manager immediately if there is a potential security breach, such as a lost or stolen laptop.
32. Employees who violate security policy are subjected to discipline, up to, and including, dismissal.
33. Service providers must notify QCOL, Inc. of any security incidents they experience, even if the incidents may not have led to an actual compromise of our data.
34. Paper records will be shredded before being placed into the trash.
35. Any data storage media will be disposed of by shredding, punching holes in, or incineration.
36. Outside contractors with access to sensitive information should be bonded.
37. Outside contractors access to sensitive information should be carefully controlled and locks and passwords changed if relationships change.
38. Change locks and passwords with employee turnovers.