1. Reviewed violations of computer security procedures and developed mitigation plans.
2. Researched and developed new computer forensic tools.
3. Developed plans to safeguard computer files against modification, destruction or disclosure.
4. Monitored computer virus reports to determine when to update virus protection systems.
5. Performed risk analyses to identify appropriate security countermeasures.
6. Encrypted data and erected firewalls to protect confidential information.
7. Conducted security audits to identify vulnerabilities.
8. Recommend improvements in security systems and procedures.
9. Monitored use of data files and regulated access to protect secure information.
10. Engineered, maintained and repaired security systems and programmable logic controls.
11. Served customers in a friendly, efficient manner following outlined steps of service.
12. Actively listened to customers, handled concerns quickly and escalated major issues to supervisor.
13. Participated in continuous improvement by generating suggestions, engaging in problem-solving activities to support teamwork.
14. Managed quality assurance program, including on-site evaluations, internal audits and customer surveys.
15. Completed all paperwork, recognizing any discrepancies and addressing them in a timely fashion.
16. Maintained and repaired facilities, equipment and tools to achieve operational readiness, safety and cleanliness.
17. Used coordination and planning skills to achieve results according to schedule.
18. Completed [task] to ensure compliance with relevant [type] regulations.
19. Used critical thinking to break down problems, evaluate solutions and make decisions.
20. Offered friendly and efficient service to all customers, handled challenging situations with ease.