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. Engineered, maintained and repaired security systems and programmable logic controls.
5. Monitored use of data files and regulated access to protect secure information.
6. Performed risk analyses to identify appropriate security countermeasures.
7. Encrypted data and erected firewalls to protect confidential information.
8. Recommend improvements in security systems and procedures.
9. Monitored computer virus reports to determine when to update virus protection systems.
10. Conducted security audits to identify vulnerabilities.
11. Saved $[amount] by implementing cost-saving initiatives that addressed long-standing problems.
12. Completed [task] to ensure compliance with relevant [type] regulations.
13. Actively listened to customers' requests, confirming full understanding before addressing concerns.
14. Used coordination and planning skills to achieve results according to schedule.
15. [Type] hardware proficiency
16. Developed team communications and information for meetings.
17. Handled [number] calls per [timeframe] to address customer inquiries and concerns.
18. Quickly learned new skills and applied them to daily tasks, improving efficiency and productivity.
19. Received and processed stock into inventory management system.
20. Actively listened to customers, handled concerns quickly and escalated major issues to supervisor.