1. Encrypted data and erected firewalls to protect confidential information.
2. Reviewed violations of computer security procedures and developed mitigation plans.
3. Monitored computer virus reports to determine when to update virus protection systems.
4. Monitored use of data files and regulated access to protect secure information.
5. Conducted security audits to identify vulnerabilities.
6. Researched and developed new computer forensic tools.
7. Recommend improvements in security systems and procedures.
8. Developed plans to safeguard computer files against modification, destruction or disclosure.
9. Engineered, maintained and repaired security systems and programmable logic controls.
10. Performed risk analyses to identify appropriate security countermeasures.
11. Used coordination and planning skills to achieve results according to schedule.
12. Increased customer satisfaction by resolving [product or service] issues.
13. Developed and implemented performance improvement strategies and plans to promote continuous improvement.
14. Developed team communications and information for meetings.
15. Maintained and repaired facilities, equipment and tools to achieve operational readiness, safety and cleanliness.
16. Worked with [type] customers to understand needs and provide excellent service.
17. Identified issues, analyzed information and provided solutions to problems.
18. Worked to maintain outstanding attendance record, consistently arriving to work ready to start immediately.
19. Actively listened to customers, handled concerns quickly and escalated major issues to supervisor.
20. Managed team of [number] employees, overseeing hiring, training, and professional growth of employees.