1. Reviewed violations of computer security procedures and developed mitigation plans.
2. Monitored computer virus reports to determine when to update virus protection systems.
3. Recommend improvements in security systems and procedures.
4. Researched and developed new computer forensic tools.
5. Monitored use of data files and regulated access to protect secure information.
6. Developed plans to safeguard computer files against modification, destruction or disclosure.
7. Performed risk analyses to identify appropriate security countermeasures.
8. Encrypted data and erected firewalls to protect confidential information.
9. Engineered, maintained and repaired security systems and programmable logic controls.
10. Conducted security audits to identify vulnerabilities.
11. Led projects and analyzed data to identify opportunities for improvement.
12. Actively listened to customers, handled concerns quickly and escalated major issues to supervisor.
13. Actively listened to customers' requests, confirming full understanding before addressing concerns.
14. Maintained and repaired facilities, equipment and tools to achieve operational readiness, safety and cleanliness.
15. Monitored all company inventory to ensure stock levels and databases were updated.
16. Completed [task] to ensure compliance with relevant [type] regulations.
17. Improved [type] through consistent hard work and dedication to [project or department or task or customer].
18. Delivered [product or service] to customer locations within specific timeframes.
19. Prepared a variety of different written communications, reports and documents to ensure smooth operations.
20. Performed duties in accordance with all applicable standards, policies and regulatory guidelines to promote safe working environment.