1. Reviewed violations of computer security procedures and developed mitigation plans.
2. Conducted security audits to identify vulnerabilities.
3. Researched and developed new computer forensic tools.
4. Recommend improvements in security systems and procedures.
5. Monitored computer virus reports to determine when to update virus protection systems.
6. Engineered, maintained and repaired security systems and programmable logic controls.
7. Performed risk analyses to identify appropriate security countermeasures.
8. Developed plans to safeguard computer files against modification, destruction or disclosure.
9. Monitored use of data files and regulated access to protect secure information.
10. Encrypted data and erected firewalls to protect confidential information.
11. Drafted detailed security policy to govern and support technology decisions.
12. Directed processes to choose, deploy and manage security software implementations.
13. Managed information system regulatory compliance to meet updated guidelines.
14. Consulted with team members to assess flawed root causes and plan for remediation.
15. Contributed system roadmapping, design and launch services to address information vulnerability.
16. Maintained excellent attendance record, consistently arriving to work on time.
17. Worked closely with [job title] to maintain optimum levels of communication to effectively and efficiently complete projects.
18. Partnered with IT department members to minimize exploits on system coverage.
19. Used coordination and planning skills to achieve results according to schedule.
20. Conducted research, gathered information from multiple sources and presented results.