1. Performed and reviewed technical security assessments of [Software] and [Software] to identify points of vulnerability and non-compliance with established information security standards and recommend mitigation strategies.
2. Developed, implemented, and documented security programs and policies and monitored compliance across departments.
3. Planned and oversaw configuration changes for security infrastructure platforms.
4. Managed [Timeframe] data center system upgrade delivering better reliability and security for server hosting and enterprise applications.
5. Applied leading theories and concepts to development, maintenance, and implementation of information security standards, procedures, and guidelines.
6. Validated and verified system security requirements definitions and analyzed system security designs.
7. Performed risk and vulnerability assessments and provided results and recommendations to senior management.
8. Counseled senior-level management on current privacy and security trends and recommendations to mitigate risk.
9. Represented company's technical security interests to partners to provide bi-directional flow of technical information and best practices in information security.
10. Delivered network system upgrade on time, under budget and with minimal service interruption.
11. Developed plans to safeguard computer files against modification, destruction or disclosure.
12. Provided consultation and technical services on all aspects of information security.
13. Provided technical leadership focused on [Area of expertise] and [Area of expertise].
14. Monitored use of data files and regulated access to protect secure information.
15. Led teams of up to [Number] in developing and implementing security systems, resulting in [Number]% fewer threats over [Timeframe].
16. Conducted security audits to identify vulnerabilities.
17. Monitored computer virus reports to determine when to update virus protection systems.
18. Researched and developed new computer forensic tools.
19. Engineered, maintained and repaired security systems and programmable logic controls.
20. Reviewed violations of computer security procedures and developed mitigation plans.