1. Monitored video surveillance feed and system alerts for suspicious activity.
2. Installed and managed video surveillance systems in [Number] buildings across [Number] companies.
3. Established company-wide security best practices and protocols to mitigate risk of data breach.
4. Provided safety reports and data analysis to building managers to inform security processes.
5. Identified, selected and deployed encryption solution to increase data protection across [Number] applications.
6. Researched and developed new computer forensic tools.
7. Outlined and maintained security patching schedule to efficiently address ongoing system issues.
8. Maintained data management and storage systems to protect data from compromise.
9. Oversaw software configurations and updates for [Number] systems across [Type] departments.
10. Completed vulnerability scans to identify at-risk systems and remediate issues.
11. Monitored use of data files and regulated access to protect secure information.
12. Reviewed violations of computer security procedures and developed mitigation plans.
13. Recommend improvements in security systems and procedures.
14. Conducted security audits to identify vulnerabilities.
15. Created and implemented security network framework across [Number] devices.
16. Encrypted data and erected firewalls to protect confidential information.
17. Developed plans to safeguard computer files against modification, destruction or disclosure.
18. Engineered, maintained and repaired security systems and programmable logic controls.
19. Decreased security incidents by [Number]% through [Action].
20. Performed risk analyses to identify appropriate security countermeasures.