1. Recommend improvements in security systems and procedures.
2. Monitored computer virus reports to determine when to update virus protection systems.
3. Conducted security audits to identify vulnerabilities.
4. Encrypted data and erected firewalls to protect confidential information.
5. Performed risk analyses to identify appropriate security countermeasures.
6. Researched and developed new computer forensic tools.
7. Engineered, maintained and repaired security systems and programmable logic controls.
8. Reviewed violations of computer security procedures and developed mitigation plans.
9. Developed plans to safeguard computer files against modification, destruction or disclosure.
10. Monitored use of data files and regulated access to protect secure information.
11. Maintained strict adherence to regulations such as payment card industry (PCI) data security standard.
12. Developed and maintained company-wide endpoint security solutions.
13. Selected appropriate Intrusion Detection System (IDS) solutions for implementation at [Type] facilities.
14. Managed company Bring Your Own Device program, onboarding employee devices and verifying absence of inherent security threats.
15. Created standardized incident response program to outline immediate and consistent remediation of security breaches.
16. Designed standardized incident logging system to track historical incursions while helping prevent future breaches.
17. Coordinated security initiatives with personnel at [Type] and [Type] sites across [Location].
18. Authored [Timeframe] security and vulnerability reports, detailing logged incursions and suggesting remediation efforts.
19. Installed and maintained commercial firewall solution, working with security vendors to consistently apply best practices and software updates.
20. Applied Center for Internet Security (CIS) benchmarks to verify performance of ongoing security measures.