1. Reviewed violations of computer security procedures and developed mitigation plans.
2. Engineered, maintained and repaired security systems and programmable logic controls.
3. Encrypted data and erected firewalls to protect confidential information.
4. Monitored computer virus reports to determine when to update virus protection systems.
5. Performed risk analyses to identify appropriate security countermeasures.
6. Recommend improvements in security systems and procedures.
7. Developed plans to safeguard computer files against modification, destruction or disclosure.
8. Researched and developed new computer forensic tools.
9. Monitored use of data files and regulated access to protect secure information.
10. Conducted security audits to identify vulnerabilities.
11. Spearheaded Bring Your Own Device program, defining necessary security parameters and designing complementary security deployments.
12. Managed relationships with third-party intrusion detection system providers.
13. Participated in creation of device hardening techniques and protocols.
14. Selected and installed company-wide [Type] security solutions.
15. Developed and maintained incident response protocols to mitigate damage and liability during security breaches.
16. Authored [Timeframe] security incident reports, highlighting breaches, vulnerabilities and remedial measures.
17. Collaborated with third-party payment card industry (PCI) compliance partners.
18. Created cybersecurity best practice communications to educate staff against known threats and potential vectors of attack.
19. Designed company-wide policies to bring operations in line with Center for Internet Security (CIS) standards.
20. Maintained company-wide compliance with industry standards such as [Area of certification].