1. Installed and maintained commercial firewall solution, working with security vendors to consistently apply best practices and software updates.
2. Created standardized incident response program to outline immediate and consistent remediation of security breaches.
3. Managed company Bring Your Own Device program, onboarding employee devices and verifying absence of inherent security threats.
4. Designed standardized incident logging system to track historical incursions while helping prevent future breaches.
5. Conducted security assessments and made recommendations for disaster recovery, remote access, network appliances, servers and directory services security.
6. Developed and maintained company-wide endpoint security solutions.
7. Administered and prepared programs for IP addresses, developed network resources and trained support personnel to provide Tier I support to end users.
8. Authored [Timeframe] security and vulnerability reports, detailing logged incursions and suggesting remediation efforts.
9. Selected appropriate Intrusion Detection System (IDS) solutions for implementation at [Type] facilities.
10. Monitored servers and escalated emergency technical issues beyond scope to maintain optimum up-time.
11. Coordinated security initiatives with personnel at [Type] and [Type] sites across [Location].
12. Maintained strict adherence to regulations such as payment card industry (PCI) data security standard.
13. Offered preventative training to harden personnel against intrusion vectors such as phishing, ransomware and more.
14. Worked with teams to develop company-wide information assurance, security standards and procedures.
15. Implemented necessary controls and procedures to protect information system assets from intentional or inadvertent modification, disclosure or destruction.
16. Coordinated with third-party security information and event management (SIEM) providers to maintain protections and predict threats.
17. Configured, managed and evaluated multi-protocol network elements for effective end-to-end communications.
18. Sustained optimal sender score on two IPs, enhancing inbox delivery and corresponding metrics while improving delivery metrics from [Number]% to [Number]%.
19. Monitored network capacity and performance, as well as diagnosed and resolved complex network problems.
20. Applied Center for Internet Security (CIS) benchmarks to verify performance of ongoing security measures.