1. Developed plans to safeguard computer files against modification, destruction or disclosure.
2. Engineered, maintained and repaired security systems and programmable logic controls.
3. Monitored computer virus reports to determine when to update virus protection systems.
4. Conducted security audits to identify vulnerabilities.
5. Recommend improvements in security systems and procedures.
6. Reviewed violations of computer security procedures and developed mitigation plans.
7. Encrypted data and erected firewalls to protect confidential information.
8. Monitored use of data files and regulated access to protect secure information.
9. Performed risk analyses to identify appropriate security countermeasures.
10. Researched and developed new computer forensic tools.
11. Led projects and analyzed data to identify opportunities for improvement.
12. Collaborated with [department or management] to achieve [result].
13. Handled day-to-day running of [project or department or task], ensuring high levels of productivity and progression.
14. Used coordination and planning skills to achieve results according to schedule.
15. Completed [task] to ensure compliance with relevant [type] regulations.
16. Worked to maintain outstanding attendance record, consistently arriving to work ready to start immediately.
17. Adhered to social distancing protocols and wore mask or face shield at all times.
18. Prepared a variety of different written communications, reports and documents to ensure smooth operations.
19. Maintained excellent attendance record, consistently arriving to work on time.
20. Managed quality assurance program, including on-site evaluations, internal audits and customer surveys.