

**ST. MARY'S COUNTY PUBLIC SCHOOLS
EXEMPT NON-CERTIFICATED POSITION DESCRIPTION**

PROJECTO COORDINATOR II – CYBER SECURITY

POSITION TITLE: Project Coordinator II - Cyber Security

REPORTS TO: Director of Information Technology and/or Supervisor of Information Technology

LOCATION: Department of Information Technology

NATURE OF WORK:

This highly skilled technical position focuses on cyber security planning, policy development, threat assessment, incident response, Artificial Intelligence (AI) controls, and data governance. The Cyber Security Engineer analyzes and strengthens SMCPs' network and data security posture while collaborating with IT teams to develop protective measures, procedures, training, and risk-reduction strategies. At this skill level, Project Coordinator II shall design Information Technology systems and solutions, ensuring their compatibility with existing infrastructure, and providing oversight for their implementation across the various facilities for which SMCPs is responsible. This requires in-depth project planning; detailed knowledge of various technologies; a firm understanding of the IT needs of SMCPs and its staff; and vendor management. This role requires expert knowledge of enterprise systems, network architecture, system integration, server administration (Linux and Microsoft), scripting/automation, and current security best practices. Work is performed under the general direction of the Director of Information Technology and/or Supervisor of Information Technology.

ESSENTIAL FUNCTIONS:

- Ability to professionally relate to and collaborate with co-workers, students, and community members
- Ability to understand and maintain confidentiality
- Ability to use technology effectively to complete tasks
- Ability to report to work daily and on time
- Ability to organize, supervise, coordinate, and establish priorities of tasks to be completed
- Ability to work independently in the absence of detailed instructions and to follow complex oral and/or written instructions
- Ability to communicate courteously and tactfully with staff, students, parents, and the community in a timely manner
- Possess excellent time management skills and the ability to take initiative and make decisions within assigned responsibility in a challenging, fast-paced professional environment and be flexible in work responsibilities and hours
- Possess knowledge of the programs, policies, and procedures of the St. Mary's County Public School
- Possess in-depth knowledge of computer networks, communication systems, database management, systems administration, enterprise systems design

DUTIES AND RESPONSIBILITIES:

- Reviews, creates, and maintains Cyber Security, AI governance, and data security documentation, standards, and policies
- Plans and implements proactive measures to enhance the district's network, data protection, and AI security posture
- Performs and oversees vulnerability assessments across all levels of SMCPs infrastructure
- Identifies, develops, and delivers tailored training for staff on cyber security, AI use, and data governance

- Conducts professional development, training sessions, tabletop exercises, and technical learning for staff on cyber security best practices, AI safety, and data management
- Oversees patching and updating of mission-critical infrastructure, including cloud, servers, networking equipment, applications, and backup systems
- Generates reports and communicates complex security, AI risk, and data governance information to stakeholders
- Demonstrates effective oral and written communication skills
- Exhibits strong interpersonal and leadership abilities
- Plans, implements, monitors, and upgrades cyber security, AI governance, and data controls
- Tests, identifies, and remediates vulnerabilities across networks, servers, applications, and AI systems
- Responds to cyber security incidents, including after-hours support as needed
- Prepares presentations, documentation, reports, and training materials for various audiences
- Compiles and formats data for security, compliance, AI risk reviews, and operational reports
- Assists with audits and reporting for regulatory compliance, including data protection and AI standards
- Maintains flexibility to accommodate a dynamic work schedule
- Performs other duties as assigned

QUALIFICATIONS:

Required:

- Bachelor's Degree **OR** Four (4) years of equivalent experience in cloud architecture, network engineering, cyber security, and/or system administration
- Knowledge and proficiency in at least one of the following scripting/automation languages:
 - Visual Basic, Python, Powershell, .Net, C#, KQL, or Java
- In addition, must possess at least one (1) of the following (please upload documentation with the application):
 - Current CompTIA Security+ Certification
 - Current CISSP Certification
 - Current CEH Certification
 - Current CISA Certification
 - Current CompTIA Network+
- Must possess a valid driver's license with no more than four (4) Maryland current points. The applicant must not be convicted, pleaded guilty or nolo contendere, or received a probation before judgment or stet docket entry for any alcohol or controlled substances offense under federal or state law for a minimum of five (5) years prior to the use of a Board-owned vehicle (Board Policy EEBA). Employee may be required to use a personal vehicle, with mileage reimbursed at the county rate, or a BoE vehicle when required to travel between locations during the same day

TERM OF EMPLOYMENT:

Full-time twelve-month position.

SALARY GRADE RANGE:

The salary for this position will be based on the EASMC-ESP salary schedule for twelve-month seven-hour employees – Range 34.

BARGAINING UNIT ELIGIBILITY: EASMC-ESP