JOB TITLE:	MANAGER DIGITAL PRIVACY AND CYBERSECURITY
DIVISION	TECHNOLOGY
SALARY SCHEDULE/GRADE:	II, GRADE 10
WORK YEAR:	220 DAYS
FLSA STATUS:	EXEMPT
JOB CLASS CODE:	0
BARGAINING UNIT:	CLAS

REVISED:

03/27/2024

Submitted:

03/26/2024

SCOPE OF RESPONSIBILITIES
Manages all procedures related to software requests throughout the district and assumes responsibility for ensuring all legal requirements are met. Manages district-wide security policies and systems. Develops, implements, and monitors the long-term information security strategy to achieve continued improvements in the district's information and systems security posture. Ensures compliance with the applicable security-related regulations, statutes, rules, and policies. Manages the JCPS Cyber Security Operations Center (CSOC) and directs the activities of that unit.

PERFORMANCE RESPONSIBILITIES & EVALUATION CRITERIA
Analyzes security metrics and other related reporting to elicit the district's information security risk profile and provides insightful advice to management for decision making
Performs enterprise-wide risk analysis and implements recommendations for application security, access control, and enterprise data safeguards to defend systems against unauthorized access, modification, or destruction
Coordinates with other IT staff as well as business units to conduct and review vulnerability security scans of systems to help identify and correct infrastructure security issues found in infrastructure and applications
Conducts district-wide awareness activities designed to assess compliance security policy education/enforcement to the entire workforce and leads committees to draft and recommend district-wide security and compliance policies and procedures
Leads the development, implementation, enforcement, and regular review of the district's information security procedures, programs, and policies
Drives the operationalization and oversees the ongoing management of the district's information security procedures, programs, and policies, holding both internal stakeholders and external vendors accountable for meeting their responsibilities
Participates in other security projects involving district information security, as needed, such as participating in compliance and risk meetings, reviewing vendor assessments for security requirements, etc
Establishes and enforces processes for developing security workflows
Coordinates, monitors, and tests the implementation of district-wide software and provides checkpoints to ensure digital privacy, safety, and security
Interfaces directly with District customers, vendors and other stakeholders and analyzes performance of the technology support services activities and documented resolutions, identifies problem areas, and devises and delivers solutions to enhance quality
Assumes responsibility for intake and fulfillment of district software vendor requests and maintaining FERPA, CIPA, COPPA, and/or other compliance requirements, regulations, and/or data protections
Works with internal and external district departments to compile and process documentation needed for data sharing agreements and contracts for software vendors
Participates in security incident responses as needed during or after business hours
Participates in projects, upgrades, outages and is available to assist after hours as needed by the team
Evaluates staff as assigned

Performs other duties as assigned by the designated supervisor
Completes all trainings and other compliance requirements as assigned and by the designated deadline
Regular, predictable performance is required for all performance responsibilities
This position requires collaboration, customer support, and team interaction

PHYSICAL DEMANDS

This work is conducted in an office setting. This position has inside environmental conditions with protection from weather conditions but not necessarily from temperature changes or atmospheric conditions while working on performance responsibilities.
This position requires the following physical activities rarely (up to 25% of the workweek): balancing, bending, climbing, crawling, crouching, driving, kneeling, and reaching. The following physical activities are required occasionally (up to 50% of the workweek): lifting up to 50 lbs., pulling up to 50 lbs., pushing up to 50 lbs., standing, and walking. Feeling, grasping, hearing, and talking are required frequently (up to 75% of the workweek). Repetitive motions and visual acuity are required constantly (up to 100% of the workweek).

MINIMUM QUALIFICATIONS

Bachelor's degree
Five (5) years of experience in Information Technology with a focus on cyber security and/or data privacy
Proficient user of technology with an understanding of risk management
Ability to lead the implementation of systems and processes to improve efficiency
Effective communication skills

DESIRABLE QUALIFICATIONS

Master's degree
A current, relevant, and industry-recognized certification or ability to complete department-designated certification(s)
Experience in a diverse workplace