INFORMATION SECURITY MANAGER

TITLE: Information Security Manager

REPORTS TO: Superintendent's Designee

SUPERVISES: Assigned Staff

JOB FUNCTION: Monitor the channels through which information flows into and out of the district's network and data systems. Responsible for observing all operations occurring across the network and data systems and managing the tools, policies, and procedures that facilitate security operations. Responsible for protecting the integrity of the FCPS network and data systems; helping develop and maintain the cybersecurity plan to protect the district against data breaches, cyberattacks, or any other information security incidents; determining cybersecurity risk; and implement appropriate mitigation planning. The Manager will secure information systems by monitoring, detecting, investigating, analyzing, and responding to security events and will take into consideration the unique structure and needs of a K-12 environment, and will use current generally accepted best practices for establishing the security environment.

MEASURES OF SUCCESS:

Annual Reviews Indicate:

- District information systems remain secure and protected.
- All district sites are current to security standards, policies, and requirements.
- Users are educated about common cyber security threats, data security, and use appropriate measures to protect district information and data.

DUTIES AND RESPONSIBILITIES:

- Work closely with district leaders to ensure that appropriate security guidance is provided to support information systems.
- Provide input into and manages the design and implementation of standards, policies, and guidelines to ensure the district's information security goals continue to be met.
- Work with other departments, as appropriate, to ensure business systems, data systems, and network infrastructure comply with the district's security requirements, state and federal guidelines, and industry best practices.
- Develop a culture of in-depth understanding as to why security testing is required at the district, school, and department level.
- Perform analysis of information protection tools, policies, and procedures and processes to identify technology security weaknesses.

INFORMATION SECURITY MANAGER

- Lead ongoing risk assessments of data processing systems to confirm the design of controls are effective and meet district, state, and federal regulatory and legal requirements.
- Develop, plan, and implement penetration testing activities to identify security weakness within the district's information system and technology environments.
- Provide quality reports to summarize test activities, including objectives, planning, methodology, results, analysis, and recommendations to both technical and non-technical audiences. From the output of the reports provide suggested approaches to enhance further.
- Provide risk analysis and recommendations for future system enhancements in line with overall district strategy.
- Recognize potential opportunities for enhancing the district's security, ensuring minimal impact to teachers, staff, students, and other users.
- Ensure district has an effective data retention and archiving process in place that conforms to state retention guidelines.
- Serve as the primary point of contact and primary escalation point for any information or data security-related issues and state breach notification requirements.
- Implement a manageable process for logging and investigating security incidents as they occur.
- Participate in and provide information for internal and external audits.
- Demonstrates the ability to communicate in more than one language or the willingness to learn to communicate in more than one language at the novice level of proficiency.
- Maintain regular attendance.
- Perform other duties as assigned.

INFORMATION SECURITY MANAGER

KNOWLEDGE AND ABILITIES:

- Broad knowledge of a wide range of Information Technology systems and a deep understanding of the inherent security risks associated with these technologies
- Understanding of information security principles and best practice
- Strong technical abilities, combined with business acumen
- Ability to present security topics to a non-technical audience and presenting the business value of security
- A good understanding of IT networking and access management concepts
- Ability to understand and assess technology systems and applications from both a technical and business function perspective
- Ability to communicate business and technical risk to all levels of audience
- Excellent interpersonal skills with the ability to build and influence teams; and self-motivated
- Ability to translate business functions into database and design concepts for the evaluation of available software
- Ability to coordinate multiple assignments, conflicting priorities, and diverse needs.

PHYSICAL DEMANDS:

- Work is performed while standing, sitting and/or walking.
- Requires the ability to communicate effectively using speech, vision, and hearing.
- Requires bending, squatting, crawling, climbing, reaching.
- Requires the ability to lift, carry, push, or pull light weights, up to 30 pounds.

EDUCATION AND EXPERIENCE:

- Bachelor's Degree in computer science, technology or business-related field.
- F ive (5) years combined successful experience in technology and cyber security.

Original Date: 11/2021

Revision Date: _____

Administrative Additive level 5