Cypress Fairbanks ISD Job Description

Security Specialist

Rev. February 2017

Job Title: Security Specialist **Wage/Hour Status: Non-Exempt**

Reports to: Chief Technology Officer **Pay Grade:** Network Specialist (WAN) IV

Dept./School: Technology Services

Primary Purpose:

Implement, enhance and oversee the Cypress Fairbanks ISD information security program including information security policies, student safety, and coordination of cybersecurity protection. Lead information security risk assessment efforts, establish a trusted learning environment to ensure privacy of student data, and drive information security awareness and training programs.

Qualifications:

Education/Certification:
Bachelor's degree in computer science or related field.
Certified Information Systems Security Professional (CISSP) preferred in certifications in one or more of the following specialty areas:

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Risk and Information Systems Control (CRISC)
- Certified Ethical Hacking (CEH)

Special Knowledge/Skills:
Knowledge of Information Security regulations including FERPA, COPPA, CIPA, and HIPAA;
Knowledge of relevant legal/regulatory requirements and common information security management frameworks such as NIST Cybersecurity Framework, ISO/IEC 27002;
Strong organizational, written and oral communication, and interpersonal skills;
Ability to implement policy and procedures;
Strong understanding of information security and the relationships among threat, vulnerability and information value in the context of risk management;
Possess a strong understanding of appropriate leading-edge technologies;
Proven successful track record in developing information security policies and procedures
Strong executive presence to be able to present analysis and recommendations in a clear and compelling manner to both technical and non-technical audiences, including executive management
Must be a critical thinker, with strong problem-solving skills
Thorough understanding of IT Operations and the role and impact of information security

Experience:
Professional experience with information security in a large complex organization;
3-5 years of progressive experience in a combination of information security, risk management, and or IT positions; and
Experience in the education industry is preferred.

Major Responsibilities and Duties:

1. Oversees the approval, training, and dissemination of security policies, standards and practices
2. Develops and enhances an information security management and control framework based on established industry standards
3. Implements security improvements by assessing current situation, evaluating trends, anticipating requirements, recognizing problems by identifying anomalies, conducting periodic audits, and reporting violations
4. Manages the framework for roles and responsibilities with regard to information ownership, classification, accountability and protection
5. Facilitates information security through the implementation of an industry best practice based governance program
6. Maintains accountability for information security program governance through the Internet Content Filtering Management Governance Committee
7. Creates and oversees the successful execution of the security roadmap including roles and responsibilities ensuring acceptable use policies.
8. Assesses overall information security risk posture, by measuring compliance with policy to ensure that security procedures are compliant with relevant laws, regulations and industry best practices, and initiates programs to achieve and maintain a successful cyber security posture.
9. Develops and maintains external and internal relationships to influence security policy, standards and programs and enhance secure interoperability with extended entities such as third-party software data interfaces
10. Leverages information security investments to enhance District administration and compliance processes.
11. Creates and manages information security and risk management communications, training and awareness programs tailored to the evolving needs of the District
12. Develop and maintain the cyber security risk assessment process, including the reporting and oversight of treatment efforts to address findings
13. Provides strategic risk guidance for IT projects and trusted learning environments including the evaluation and recommendation of technical controls and solutions
14. Works with the appropriate District resources to monitor the external threat environment for emerging threats, and advises relevant stakeholders on the appropriate courses of action
15. Leads the development and management of a comprehensive Threat and Vulnerability Management program
16. Oversees cyber security incident response capabilities, and directs enhancements to align with industry standards
17. Performs other duties as assigned by the Chief Information Officer

Working Conditions:

Mental Demands/Physical Demands/Environmental Factors:
Frequent districtwide travel and occasional statewide travel; occasional prolonged and irregular hours.

The foregoing statements describe the general purpose and responsibilities assigned to this job and are not an exhaustive list of all responsibilities and duties that may be assigned or skills that may be required.

Approved by _____ Date _____

Reviewed by _____ Date _____