

JOB DESCRIPTION

Job Title Technology Security Administrator
Reports to Manager, Technology Security Office
Dept/School Information Technology

Job Title Code 182421
Wage/Hour Status Exempt
Pay Grade 505
Date Revised April 10, 2025

Primary Purpose

Administer the district's technology, information, and cybersecurity programs and processes to ensure a secure, compliant, and protected technology environment. Responsible for daily operations related to cybersecurity monitoring, incident response, risk management, regulatory compliance, and security architecture. Support the identification, evaluation, and reporting of technology security risks and assist with the design and implementation of effective safeguards and enterprise-wide security strategies. Maintain 24/7 monitoring and compliance across all technology security office operations.

Education/Certification

- Bachelor's degree in Computer Science, Cybersecurity, Information Technology, or a related field required, and five (5) years' experience in Cybersecurity, Public Safety, Emergency Management, Engineering, Information & Technology Security, Security Communications, or related field.
OR
- Associate degree in information & technology security or related field and (7) years' experience in Cybersecurity, Public Safety, Emergency Management, Engineering, Information & Technology Security, Security Communications, or related field.
OR
- High school diploma/GED and nine (9) years' experience in cybersecurity, public safety, technology & information security, security communications, surveillance, telecommunications, & contingency systems.
- Technical certification(s) such as Certified Information Systems Security Professional (CISSP), CompTIA Security+, CompTIA Advanced Security Practitioner (CASP), or CCNA-Security certification or similar specialized in technology, networking and/or electronic security coursework may be substituted for two (2) years of experience.
- Valid Texas/New Mexico driver's license, insurable by the district's auto liability insurance carrier; subject to district's drug and alcohol screening policy and regulation.
- Must maintain valid certifications, as required & determined, for the district's technology, safety & security systems, and programs.

Special Knowledge/Skills

- In-depth knowledge of cybersecurity principles, security operations, risk management, and incident response
- Solid understanding with regulatory frameworks and standards such as NIST, ISO 27001, CIPA, FERPA, and HIPAA
- Knowledge of IST technologies and common information security management frameworks (i.e. ISO/IEC 27001, ITIL, NIST, COBIT, etc.), penetration testing and ethical hacking
- Hands-on experience with security technologies such as firewalls, IDS/IPS, endpoint protection, SIEM, and authentication systems
- Strong understanding of security networking concepts (TCP/IP, VLANs, VPNs, DNS, DHCP)
- Demonstrate knowledge in security administration and configuration to include work in multiple operating systems and network protocols (i.e., WINDOWS, NT, UNIX, MS-DOS, LINUX, VMware, Chrome, IOS and MAC-OS), (TCP/IP, SNMP, DHCP, DNS, SFTP, HTTP, LDAP); infrastructure monitoring tools (FLUKE, Solar Winds), internet services (DNS, WWW & FTP), INFOBLOX and emerging technologies

JOB DESCRIPTION

- Advanced knowledge in Perimeter Firewall (i.e., Palo Alto), Web Content Filter Appliance, infrastructure security, Remote Access, and configuration
- Knowledge with VMware server infrastructure, Microsoft Networking, Windows server operating systems Domain, Active Directory, Exchange technologies, Printing, INTUNE, AZURE, storage sub-systems, SAN, e-mail administration, sandboxing, security management products, group policy, workstation, database, and support systems
- Experience using Google Apps, JAMF Administration mobile device management, security configuration and policy management, MS Windows, OFC365, Google, and Apple systems.
- Ability to analyze complex security issues and recommend effective solutions
- Team player with strong interpersonal skills and ability to collaborate with a diverse group of individuals at all levels of the district and with cross-functional teams and exercise independent judgment and discretion in carrying out duties and responsibilities
- Evident focus on customer service initiatives, rigor and discipline, teamwork, collaboration, personal and professional responsibilities, staff development and training
- Excellent written and verbal communication and presentation skills with the ability to make technical issues understandable to a wide-ranging audience

Major Responsibilities and Duties

Technology and Cybersecurity Program Administration

1. Administer the district's cybersecurity policies, frameworks, and daily operations to ensure the confidentiality, integrity, and availability of all technology systems and services.
2. Oversee monitoring tools and platforms to ensure continuous protection against threats, vulnerabilities, and breaches.
3. Work with District Security teams, federal, state, and local public safety entities on district/campus emergency and safety communications systems planning & management to include law enforcement and first responders.
4. Process requests to grant computer and/or network access privileges that have been approved by designated members of management or data owners.
5. Evaluate requests for change for any configurable items that may affect the confidentiality, integrity or availability of District's applications.

Threat Monitoring and Incident Response

6. Conduct real-time 24/7 monitoring of network and security system events.
7. Investigate security incidents, analyze breaches, contain threats, and lead remediation efforts.
8. Develop and maintain incident response plans and assist in forensic investigations when necessary.

Risk Assessment and Management

9. Perform regular vulnerability assessments, penetration testing, and risk evaluations of district systems and networks.
10. Analyze security risks and recommend appropriate mitigation strategies and security improvements.
11. Maintain risk management documentation and support risk-related audits and reporting.
12. Develop and support the development of automated mechanisms that analyze the security violations found in access control logs to discover patterns and evidence of problems.

Security Controls and Safeguard Implementation

13. Assist in the design, implementation, and maintenance of enterprise-wide security controls and safeguard measures.
14. Administer and support cybersecurity systems such as firewalls, antivirus/antimalware platforms, endpoint protection, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), web content filters, multi-factor authentication (MFA), VPNs, and encryption tools.
15. Assist with technical security related equipment and controls, including access controls, smart devices, intrusion detection, communications systems, panic buttons, surveillance cameras and equipment needed for full operability of the district's physical security systems.

JOB DESCRIPTION

16. Ensure systems are securely configured and aligned with cybersecurity frameworks and best practices.

Compliance and Regulatory Requirements

17. Ensure the district's technology systems and practices comply with applicable laws, regulations, and standards, including FERPA, CIPA, HIPAA, and relevant state/federal cybersecurity regulations.
18. Assist with security audits and regulatory reviews and coordinate the collection of compliance evidence.
19. Maintain up-to-date documentation on compliance initiatives and security practices.

Policy Development and Security Awareness

20. Assist in creating and updating cybersecurity policies, procedures, and standards.
21. Promote cybersecurity awareness among district employees and students through ongoing education, training sessions, and communication initiatives.
22. Serve as a resource for interpreting cybersecurity requirements and best practices for all stakeholders.

Collaboration and Security Integration

23. Collaborate with IST leadership, technology administrators, engineers, and application teams to integrate security into technology projects and operations.
24. Provide guidance to technical teams on secure system designs and cybersecurity best practices.
25. Participate in district-wide technology planning and decision-making activities related to cybersecurity.

Monitoring, Reporting, and Continuous Improvement

26. Develop and maintain dashboards, reports, and metrics that track the district's cybersecurity posture.
27. Continuously review and enhance security practices, tools, and processes based on emerging threats and industry standards.
28. Stay informed on the latest cybersecurity threats, vulnerabilities, and mitigation strategies.

Other Responsibilities

29. Sustain and adheres to IT Professional's Code of Ethics and Standards of Conduct.
30. Liaise with external agencies, law enforcement and other advisory bodies as necessary, to ensure the district maintains a strong security posture.
31. Participate in development, implementation, and testing of a disaster recovery plan, intrusion and other security assessments and serve as a member of the district contingency task force.
32. Attend professional & leadership growth opportunities and maintain a broad and current knowledge of emerging technology, innovation, equipment, and systems.
33. Provide optimal customer services to all students, employees, parents, community members and stakeholders and assists in community awareness of district technological goals and programs.
34. Support the goals and objectives of the district and comply with policies established by federal and state law, State Board of Education rules, and local board policy.
35. Uphold and adheres to safety rules and polices of the EPISD ISD safety program.
36. Attend work on a regular and routine basis to avoid disruption to district technology operations.
37. Perform other appropriate duties, as assigned.

Supervisory Responsibilities

May assist in personnel supervision as assigned.

Physical and Mental Job Requirements

Mental Demands/Physical Demands/Environmental Factors

- Maintain emotional control under stress. Repetitive hand motions and prolonged use of the computer. Frequent district-wide travel. Occasional prolonged and irregular hours, with availability for emergency coverage. Work with frequent interruptions. After-hours/holiday/weekend work for upgrades, maintenance, troubleshooting and projects. Must be able to lift, carry, push and/or pull up



JOB DESCRIPTION

to fifty (50) pounds frequently; work under inclement weather conditions; exposure to extreme temperatures, chemicals and loud noises; be adaptable to work a shift schedule and/or hours than regularly assigned; extended periods of walking, standing, bending, reaching, kneeling, stooping, heavy lifting and carrying. Work indoors and outdoors. and around moving objects or vehicles; ladders or scaffolding.

Terms of Employment

226 days; salary to be established by the Board of Trustees

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: _____
Job Title: _____
Date: _____

Approved: _____
Job Title: _____
Date: _____

My supervisor has reviewed this job description with me and has provided me with a copy.

Employee: _____
Date: _____

The El Paso Independent School District does not discriminate in its educational programs or employment practices on the basis of race, color, age, sex, religion, national origin, marital status, citizenship, military status, disability, genetic information, gender stereotyping and perceived sexuality, or on any other basis prohibited by law. Inquiries concerning the application of Titles VI, VII, IX, and Section 504 may be referred to the District compliance officer, at 230 -2031; Section 504 inquiries regarding students may be referred to 504 Coordinator at 230-2856.

El Distrito Escolar Independiente de El Paso no discrimina en los programas de educación o en prácticas de empleo usando el criterio de raza, color, edad, sexo, religión, origen nacional, estado civil, ciudadanía, estado militar, discapacidad, información genética, estereotipo sexual o sexualidad percibida, u otra práctica prohibida por la ley. Preguntas acerca de la aplicación del título VI, VII o IX, y la Sección 504 pueden ser referidas al oficial del distrito, al 230-2031; preguntas sobre 504 tocante a estudiantes pueden ser referidas al oficial de 504 al, 230-2856.