JOB TITLE: TECHNOLOGY COORDINATOR

REPORTS TO: Director of Teaching and Learning

EVALUATION: Annual performance review in accordance with Board of Education Policy.

PURPOSE: The Technology Coordinator serves as the senior technical resource responsible for the administration, architecture, reliability, and security of the District's technology infrastructure. This role leads the design, configuration, maintenance, and troubleshooting of on-premises servers, network/wireless systems (LAN/WAN), firewalls, and cloud-integrated platforms, ensuring systems are scalable and aligned with instructional needs.

ESSENTIAL JOB FUNCTIONS

I. Leadership, Strategic Planning, & Governance

- **Departmental Leadership:** Directs and evaluates Technology Specialists, establishing annual departmental goals and performance metrics.
- **Strategic Collaboration:** Works with district leadership and the Director of Teaching and Learning to align technology initiatives with curriculum goals, identifying budget requirements and funding mechanisms to ensure improved student outcomes.
- **Process Formalization:** Develops and maintains formally documented, repeatable procedures for all technical operations—including asset lifecycles, vulnerability management, and audit log reviews—to ensure audit-defensibility and operational consistency.
- **Priority Setting:** Facilitates the process of priority setting for the district's data analysis needs and monitors departmental progress toward strategic goals.

II. Network, Infrastructure, & Asset Management

- **Systems Lifecycle:** Oversees the installation, maintenance, and long-term enhancement of all district network infrastructure, server equipment, and computing devices (including iPads, Chromebooks, and Mac computers).
- **Service & Integration:** Administers authentication services, virtualization, and system integrations; supports the on-premises Student Information System (SIS) in coordination with remote vendor support.
- **Automated Asset Management:** Oversees accurate inventories using automated tools (e.g., Incident IQ, Jamf, Google Admin) and implements a weekly process to identify, review, and quarantine unauthorized devices on the network.
- **Digital Presence:** Implements procedures to maintain and update the district's web presence and communication tools, ensuring all resources remain operational and relevant.

III. Security, Privacy, & Compliance

- **Data Governance:** Establishes a documented data management process that defines sensitivity levels, ownership, and secure disposal protocols (e.g., NIST 800-88 sanitization) for all District data.

- **Advanced Protections:** Manages all cybersecurity aspects, including the enforcement of Multi-Factor Authentication (MFA), encryption-at-rest (AES-256) for sensitive data, and the management of default vendor/administrative accounts.
- **Vulnerability & Audit Management:** Operates a recurring vulnerability management program—utilizing quarterly authenticated/unauthenticated scans and CVSS risk prioritization—and maintains a centralized log review process to detect unauthorized activity.
- **Incident Response:** Acts as the lead for the Security Incident Response Team (SIRT), maintaining documented playbooks, escalation paths, and public reporting mechanisms for security events.
- **Legal Compliance:** Models and ensures district adherence to all state and federal laws, specifically including SOPPA, FERPA, CIPA, E-rate, and copyright regulations.

IV. Instructional Support & Professional Development

- **Assessment Oversight:** Provides technical leadership and infrastructure support for state and local assessments, including WIDA, KIDS, IAR, ACCESS, and i-Ready.
- **Strategic PD Plan:** Collaborates with leadership to develop and execute a strategic professional development plan for education technology and proficient tech use by staff and students.
- **Security Awareness Program:** Designs and manages a mandatory, recurring Security Awareness Program for all employees—including phishing simulations and authentication training—to foster a "security-first" culture.

V. Financial Management & Vendor Oversight

- **Revenue Generation:** Identifies and secures diverse funding sources, including E-rate applications, grants, state funding, and community partnerships.
- **Fiscal Sustainability:** Guides purchasing decisions, determines return on investment (ROI) for implementations, and pursues cost-reduction or cost-shifting measures.
- **Third-Party Risk Management:** Conducts annual security reviews of service provider contracts to ensure they include specific requirements for breach notification, data encryption, and disposal commitments.

MINIMUM QUALIFICATIONS

- **Education:** Degree in Instructional Technology, Computer Science, or a related field.
- **Experience:** Minimum of 3–5 years in a technology leadership role, including staff management and budgeting.
- **Technical Expertise:** Expertise in network administration (servers, infrastructure, security), Google Workspace, and SIS management.
    - Working knowledge of CVSS (Common Vulnerability Scoring System) and encryption protocols (AES-256).
    - Ability to conduct security audits of service provider contracts.
- **Attributes:** Strong analytical troubleshooting skills; ability to translate complex technical concepts for non-technical stakeholders; ability to lift and carry up to 20 lbs and push/pull up to 10 lbs

CONTRACT: 12-month
COMPENSATION: $90,000-$105,000