POSITION TITLE:

SYSTEM ADMINISTRATOR

Reports to: Supervisor of Technology

Function/Purpose:
To provide technical ownership, administration, architecture, security, and lifecycle management for the Division's enterprise systems, cloud platforms, identity services, endpoint environments, automation technologies, and related technology services.

General Description:
The System Administrator serves as the technical owner of enterprise systems and platforms. This role is responsible for system architecture, configuration standards, security posture, automation strategy, disaster recovery planning, and long-term platform sustainability. While the position may participate in operational activities when required, its primary purpose is technical ownership, planning, standards development, and architecture rather than routine support or operational execution.

Required Education, Knowledge, Qualification and Experience:

- A wide range of experience and knowledge of technology and its applications.
- A combination of relevant post-secondary education, industry certifications, training, and demonstrated enterprise technology experience.
- Experience or knowledge in enterprise systems, server and cloud platforms, identity and access management, endpoint management, cybersecurity controls, automation solutions, monitoring systems, and related technology platforms will be considered an asset.

Required Skills and Abilities:
Demonstrated capability and performance in the areas of:

- Ability to work independently with minimal supervision, exercise sound professional judgment, take initiative, and be accountable for the quality and completion of assigned work.
- Ability to assess technical, operational, cybersecurity, continuity, and enterprise system risks and recommend appropriate mitigation measures.
- Ability to plan, design, configure, administer, maintain, and support secure, reliable, resilient, and sustainable enterprise systems and technology platforms.
- Ability to research, evaluate, test, and recommend technology solutions based on operational requirements, security, compatibility, sustainability, and long-term value.
- Ability to develop, maintain, and apply technical standards, procedures, configuration requirements, system documentation, and related records.
- Ability to analyze system performance, platform telemetry, security events, logs, alerts, and monitoring information to identify operational issues, emerging risks, and security concerns.
- Ability to investigate complex system, endpoint, identity, cloud, and security-related incidents and coordinate appropriate containment, remediation, recovery, root-cause analysis, and follow-up activities.

- Ability to design, develop, maintain, and evaluate automation, scripting, system integration, configuration, deployment, and administrative solutions.
- Ability to organize and prioritize multiple operational demands, incidents, projects, maintenance requirements, and platform initiatives based on urgency, risk, and organizational impact.
- Ability to plan, maintain, test, and document backup, disaster recovery, business continuity, and system resiliency requirements.
- Ability to coordinate technical projects and system initiatives involving IT staff, schools, departments, vendors, service providers, and security partners.
- Ability to provide clear technical direction, guidance, mentorship, and implementation support to staff performing enterprise system, identity, endpoint, cloud, security, automation, and related technology work.
- Ability to communicate technical information clearly and effectively, both verbally and in writing, and adapt explanations to the technical understanding of the audience.
- Excellent interpersonal, communication, and collaborative skills, including the ability to work effectively and respectfully with staff, students, administrators, IT staff, vendors, service providers, and other stakeholders.
- Ability to recognize issues requiring supervisory, policy, financial, risk-acceptance, or organizational decisions and escalate them appropriately.
- Ability to maintain accurate system records, inventories, configuration information, technical documentation, standards, procedures, and change records.
- Ability to exercise discretion and appropriately handle confidential, sensitive, security-related, and operational information.
- Ability to adapt to changing priorities, incidents, outages, emerging threats, operational demands, and evolving technology requirements.
- Ability and willingness to continually develop technical knowledge and skills as enterprise systems, cloud services, identity platforms, endpoint technologies, cybersecurity controls, and automation solutions evolve.

Required Personal Characteristics:

- Trustworthy and respectful.
- Approachable and accessible.
- Flexible and collaborative.

Supervision:

The System Administrators will not generally be required to directly supervise employees. The System Administrator may provide technical direction and guidance within approved standards and assigned projects but does not exercise supervisory authority with respect to employee performance, discipline, scheduling, or other personnel matters unless specifically delegated by the Supervisor of Technology

General Duties:

- Be willing to engage in lifelong learning with respect to training, in-service, and courses of study.
- Conduct oneself in a manner appropriate for an individual employed by an educational system that provides services to children.
- Deal tactfully with staff, students, administration, and the public.
- Be knowledgeable and supportive of applicable Board policies.
- Organize, carry out, and assist in technology activities across the Division under the direction of the Supervisor of Technology, with primary responsibility for enterprise systems, cloud services, identity and access management, endpoint management, automation technologies, and related security platforms.
- Plan, design, configure, administer, maintain, and continually improve secure, reliable, resilient, and sustainable enterprise systems and technology platforms.
- Establish and maintain system architecture, configuration standards, administrative controls, identity and access requirements, endpoint standards, system integrations, and related cybersecurity controls.
- Administer and maintain enterprise server, cloud, identity, endpoint management, monitoring, automation, backup, recovery, and related technology platforms.
- Monitor and analyze system health, platform performance, security alerts, logs, telemetry, configuration information, and monitoring data to identify operational issues, security concerns, emerging risks, and opportunities for improvement.
- Lead or participate in the investigation, containment, remediation, recovery, root-cause analysis, and documentation of system-related incidents, outages, security events, and service disruptions.
- Review system, endpoint, identity, and cloud-related vulnerability findings; assess operational and cybersecurity exposure; establish remediation priorities; and implement or coordinate approved corrective actions.
- Define and maintain patching, system maintenance, configuration management, system-hardening, and lifecycle-management strategies for enterprise systems, endpoints, cloud services, identity platforms, and related technologies.
- Design, develop, maintain, test, and continually improve automation, scripting, integration, deployment, configuration, and administrative solutions.
- Develop, maintain, test, and document disaster recovery, business continuity, backup and recovery, and resiliency plans relating to enterprise systems and technology platforms.
- Maintain accurate and authoritative system documentation, inventories, diagrams, configuration records, standards, procedures, baselines, and change records.
- Research, evaluate, test, and recommend enterprise system, cloud, identity, endpoint, cybersecurity, automation, monitoring, backup, and recovery technologies based on operational requirements, risk, compatibility, sustainability, and long-term value.

- Coordinate with the Network Administrator, IT Service Technicians, schools, departments, vendors, service providers, and security partners to ensure enterprise technology services remain reliable, secure, sustainable, and effective.
- Provide technical direction, approved standards, escalation support, and implementation guidance to staff performing enterprise system, cloud, identity, endpoint, security, automation, and related technology work.
- Validate significant system changes and completed technical work to ensure alignment with approved architecture, security controls, configuration standards, documentation requirements, and operational expectations.
- Participate in meetings, planning activities, projects, in-services, and professional learning as required.
- Provide technical advice, information, and training to staff as required.
- Maintain all required records and documentation.
- Comply with applicable laws, Board policies, administrative procedures, professional expectations, and confidentiality requirements.
- Perform other related duties as assigned.

Ordering Materials:
The System Administrator may initiate or recommend purchases of approved materials, equipment, software, and services required to maintain enterprise systems and technology platforms. Purchases must follow Division purchasing procedures and receive approval from the Supervisor of Technology or designated authority.

Judgment, Independence & Client Contact:
- Confidentiality
    - A System Administrator is expected to respect the confidential nature of the position by avoiding discussion of any topics that are not formally communicated to the public by the administration of the school or the Division. Information regarding a student, staff member or Board member must not be discussed in public or with any person not authorized to receive that information. Exchange of personal information within the system shall be on a “need to know” basis. Breaching confidentiality is a serious violation of acceptable conduct and is grounds for disciplinary action up to and including termination of employment with the Board.
- Independence
    - The System Administrator is expected to work independently, take initiative and be responsible for quality of assigned work.
- Working Jointly with Other Staff on Common Assignments or Tasks
    - This position involves working jointly with other staff, teachers and school-based administration on a daily basis.

New appointees will undergo a ten (10) month probationary period.

Mission: Laying the foundation for success.
Vision: One student at a time.

Revised: October 2021
Revised: August 2015
Director Approved: November 10, 2026