CCSD
CLARK COUNTY
SCHOOL DISTRICT

Identity and Access Management Analyst

Position Details

Class Code: 1442
Job Family: Information Systems
Classification: Support Professional
Terms of Employment: Pay Grade 58 on the Support Professional Salary Schedule
FLSA STATUS: NON-EXEMPT

Position Summary

Under general supervision, this position is responsible for managing and maintaining the Clark County School District (CCSD)’s identity and access management systems. This role involves ensuring secure access to systems and data, implementing identity and access management (IAM) policies and procedures, and providing support for identity-related issues.

Essential Duties and Responsibilities

The list of Essential Duties and Responsibilities is not exhaustive and may be supplemented.

1. Manages user account lifecycle processes, including onboarding, modifications, and offboarding, ensuring timely and accurate access rights.
2. Implements role-based access control (RBAC) and ensure compliance with the principle of least privilege.
3. Configures and maintains access control policies and settings within IAM systems to align with CCSD requirements.
4. Conducts regular reviews and audits of user access rights to ensure compliance and identify any discrepancies.
5. Monitors and maintain IAM tools and technologies, ensuring optimal performance and security.

6. Implements updates, patches, and enhancements to IAM systems as required.
7. Responds to access-related incidents and security breaches, conducting investigations and coordinating remediation efforts.
8. Documents incident findings and maintain accurate records of all actions taken.
9. Assists in the development and implementation of IAM policies, standards, and procedures to support security and compliance objectives.
10. Ensures adherence to regulatory requirements and best practices related to IAM.
11. Provides technical support to end-users regarding IAM systems, access issues, and identity-related inquiries.
12. Conducts training sessions for employees on IAM policies, procedures, and best practices to enhance security awareness.
13. Generates and maintains reports on user access, compliance metrics, and IAM system performance for management review.
14. Documents IAM processes, configurations, and user guides to facilitate knowledge sharing and operational continuity.
15. Conforms to safety standards, as prescribed.
16. Performs other tasks related to the position, as assigned.

Distinguishing Characteristics

Responsible for implementing and managing identity and access control protocols to secure network resources. Configures, monitors, and maintains access management systems, including single sign-on (SSO), multi-factor authentication (MFA), and role-based access control (RBAC) solutions. Supports the provisioning and de-provisioning of user accounts, regularly reviews access privileges, and addresses access-related incidents. Assists in the analysis of access logs and performs periodic audits to ensure compliance with security policies and regulatory standards, contributing to a secure and well-managed user identity environment.

Knowledge, Skills, and Abilities (Position Expectations)

1. Knowledge of regulatory requirements related to identity and access management (e.g., General Data Protection Regulation [GDPR], Health Insurance Portability and Accountability Act [HIPAA]).
2. Strong understanding of IAM concepts, practices, and frameworks.
3. Excellent problem-solving skills and attention to detail.

4. Strong communication and interpersonal skills, with the ability to work effectively with technical and non-technical stakeholders.
5. Ability to recognize and report hazards and apply safe work methods.
6. Possess physical and mental stamina commensurate with the responsibilities of the position.

Position Requirements

Education, Training, and Experience

1. High school graduation or other equivalent (General Educational Development [GED], foreign equivalency, etc.).
2. Two (2) years of college courses in computer science or information security from an accredited college or university; and, two (2) years of experience supporting/operating telecommunications and networking security, application and systems security, application development security, user authentication and authorization management, information systems vulnerability assessment, and physical data security, with supervision of technical staff; or,
   Bachelor's degree from an accredited college or university in Computer Science, Information Technology, Cybersecurity, or a related field.

Licenses and Certifications

1. A valid driver's license that allows the applicant/employee to legally operate a motor vehicle in Nevada. License must be maintained for the duration of the assignment.
2. Current driving history (dated within six [6] months from the date printed) issued by the Department of Motor Vehicles (DMV) at the time of application or Qualified Selection Pool (QSP) placement and at the time of interview prior to final selection.
3. Safe driving record. Safe driving record must be maintained for the duration of the assignment.

Preferred Qualifications

1. Two (2) to five (5) years of experience in IAM, IT security, or a related field.
2. Familiarity with IAM tools and technologies, such as Identity Governance and Administration (IGA) and SSO.
3. Experience with IAM system implementation and administration.
4. Familiarity with cloud-based IAM solutions and identity federation.

5. Prior experience in a regulated industry (e.g., finance, healthcare) is advantageous.

Document(s) Required at Time of Application

1. High school transcript or other equivalent (GED, foreign equivalency, etc.).
2. College transcripts from an accredited college or university.
3. Copy of a valid driver's license that allows the applicant/employee to legally operate a motor vehicle in Nevada.
4. Copy of current driving history (dated within six [6] months from the date printed) issued by the DMV.
5. Safe driving record.
6. Specific documented evidence of training and experience to satisfy qualifications.

Examples of Assigned Work Areas

Enterprise Information Security Department, and travel to and from schools and other CCSD office settings.

Work Environment

Strength

Sedentary/light - exert force up to 20 lbs., occasionally; 10 lbs., frequently; negligible force, constantly.

Physical Demand

Frequent sitting, standing, walking, pushing, pulling, stooping, kneeling, crouching, reaching, handling, and repetitive fine motor activities. Hearing and speech to communicate in person, via video conference and computers, or over the telephone. Mobility to work in a typical office setting and use standard office equipment. Stamina to remain seated and maintain concentration for an extended period of time. Vision: Frequent near acuity, occasional far acuity, and color vision. Vision to read printed and online materials, Video Display Terminal screens, or other monitoring devices.

Environmental Conditions

Climate-controlled office setting with temperatures ranging from mild to moderate cold/heat. Exposure to noise levels ranging from moderate to loud for occasional to frequent time periods.

Hazards

Furniture, office equipment, communicable diseases, chemicals and fumes (as related to specific assignment), and power/hand-operated equipment and machinery (as related to specific assignment).

Examples of Equipment/Supplies Used to Perform Tasks

CCSD-issued/personal vehicles, various computers, printers, copiers, calculators, fax machines, telephones, filing cabinets/equipment, etc.

AA/EOE Statement

The Clark County School District is proud to be an equal opportunity employer. The Clark County School District is committed to providing all applicants and employees equal employment opportunities without regard to race, color, religion, sex, gender identity or expression, sexual orientation, national origin, genetics, disability, age, military status, or other characteristics protected by applicable law. Here at Clark County School District, we are a diverse group of people who honor the differences that drive innovative solutions to meet the needs of our students and employees. We believe that through a culture of inclusivity, we have the power to reflect the community we serve.

Job Revision Information

- Created: 02/19/25