RESOLUTION NO. 2023- 8819

RESOLUTION TO AMEND FISCAL YEAR 2022-2023 JOB CLASSIFICATION PLAN ADDING TWO NEW JOB CLASSIFICATIONS TO INFORMATION TECHNOLOGIES DEPARTMENT #20220

WHEREAS, Plumas County Personnel Rule 5.01 provides amendments to be made by resolution of the Fiscal Year 2022/2023 Job Classification Plan covering all positions in the County service; and

WHEREAS, these positions are necessary in the daily operational needs of the Information Technologies Department Fund #20220; and

WHEREAS, this request was brought to the attention of the Human Resources Director who is now requesting approval of this resolution to amend the 2022-2023 Position Allocation adding two (2) new job descriptions for a SAAS Systems Administrator with a base wage of $29.78 and Network/EDR Administrator base wage of $27.65 job descriptions, Fund #20220; and

WHEREAS, Plumas County has met the meet and confer obligations for this position with Confidential Unit; and

**NOW, THEREFORE BE IT RESOLVED** by the Plumas County Board of Supervisors as follows:

Approve the attached two (2) new job classifications for the positions of Plumas County SAAS Systems Administrator base wage of $29.78 and Network/EDR Administrator base wage of $27.65 and add these new classifications to the Confidential Unit based confidential definition of these position.

The foregoing Resolution was duly passed and adopted by the Board of Supervisors of the County of Plumas, State of California, at a regular meeting of said Board on the 30th day of June 2023 by the following vote:

AYES: Supervisors: Engel, Goss, Hagwood, McGowan, Ceresola

NOES: Supervisors: None

ABSENT: Supervisors: None
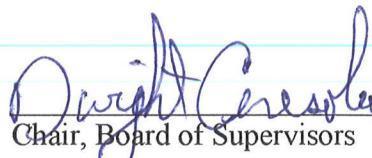
Chair, Board of Supervisors
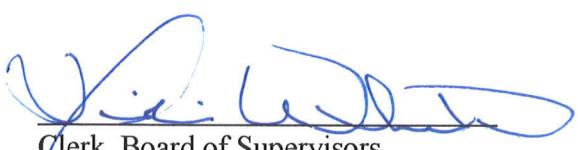
Clerk, Board of Supervisors

NETWORK /EDR ADMINISTRATOR

DEFINITION

Under general direction of the Director of Information Technology to configure, maintain, and administer all County networks and EDR (endpoint detection & response) tools used by all County departments; and to perform related and other duties as required.

DISTINGUISHING CHARACTERISTICS

A Network/EDR Administrator is responsible for overseeing an organization's database networks to ensure proper maintenance and cybersecurity. Identifies threats to security and acts as lead on support response to the EDR platform. Duties include working with other IT staff and County employees to identify network or computer system needs, overseeing the installation of new hardware or software and using employee feedback to isolate issues. This position has access and supports the County's financial and personnel systems with access to confidential information.

This position analyzes and monitors all ongoing activities for devices connected to the County's network and provides real-time threat detection and visibility for automated threat response for security teams for cybersecurity.

REPORTS TO

Director of Informational Technology

CLASSIFICATIONS DIRECTLY SUPERVISED

None

EXAMPLES OF DUTIES

- Administers and optimizes all County networks, troubleshooting and resolving network issues, implementing cybersecurity measures, and proactively optimizing network performance.
- Maintaining computer networks and systems including software, mainframes, VPNs, routers and other physical hardware.
- Combine and correlate full-spectrum endpoint visibility data across al devices to analyze activity and provide details about Indicators of Compromise (loC) as well as Indicators of Attack (IoA).
- Installing and configuring network equipment to update or fix hardware or software issues.
- Updating virus protection software to keep data and communications protected.
- Monitoring computer systems to improve network performance for computer systems and networks.
- Communicating networking issues to other employees and management, especially in training new users.
- Fixing software and hardware configuration issues for users on-demand or from inspection of the systems.
- Administers and optimizes County EDR (endpoint detections & response) tools.
- Administers county data backups and related tools.
- Works with state entities / vendors to understand network requirements and determines best practices to facilitate those needs while complying with county policies.
- Prepares thorough topologies and documentation on County networks.
- Prepares thorough and clear documentation on County EDR tools.
- Prepares & hardens county endpoint operating systems.
- Monitors new security risks and prepares reports / dashboards on these risks for the Information Technology Director.
- Continually monitor for necessary updates, ensuring optimal network performance and security.
- Installs and tests new computer hardware, software, and operating systems.
- Assists with county desktop support.
- Perform related duties as assigned.

TYPICAL PHYSICAL REQUIREMENTS

Sit for extended periods; frequently stand and walk; normal manual dexterity and eye-hand coordination; some kneeling and stooping; physical ability to lift and move objects weighing up to 50 lbs.; corrected hearing and vision to normal range; verbal communication; use of office equipment including computers, telephones, calculators, copiers, and FAX.

TYPICAL WORKING CONDITIONS

Work is performed in an office environment; some exposure to dust and electrical energy; continuous contact with staff and the public.

DESIRABLE QUALIFICATIONS

Knowledge of:

- Analyzing and figuring out the systems needs of a government County agency.
- Use of various data analytics techniques to detect suspicious system behavior.
- Installing hardware and software for the network.
- Antivirus (AV) and antimalware (AM) tools.
- Advanced threat detection and malicious activity detection.
- Containment of the cyber security threat at the compromised endpoint.
- Incident data search and investigations – alert triage with high fidelity alerting.
- Suspicious activity and remediation guidance.
- Threat hunting to protect the endpoint against future attacks.
- Keeping systems operating efficiently by performing any necessary upgrades and repairs.
- Planning a strategy to maintain system security on the computers and the network.
- Optimizing and evaluating the system regularly.
- Assigning and updating security permissions for the system network.
- Training or directing users on the correct use of software and hardware within the system.
- Performing problem-solving tasks when alerted by an employee user or monitoring system.
- Computer operating systems.

Ability to:

- Analyze user information system needs and develop systems to meet those needs.
- Proactively monitor, detect, and remediate or isolate threats on endpoint devices as they happen.
- Focus on endpoint security as a key part of the overall County's IT security strategy.
- Lead and oversee deployment, operation, and maintenance of the global EDR platform.
- Block malicious activities throughout the County's computer systems.
- Detect to contain, investigate, and eliminate invasive cybersecurity threats.
- Provide remediation options in response to threats to restore affected systems.
- Evaluate and prioritize projects under the direction of the Information Technology Director.
- Maintain the confidentiality at all times
- Communicate clearly and concisely, both orally and in writing.

Training and Experience:

A minimum of two (2) years' experience in TCP/IP, Cisco Training, familiarity with backup and recovery software and methodologies, and computer & server operating systems.

Specific knowledge of Cisco Meraki Administration, Firewall Configuration, Cohesity Backup Administration, Crowdstrike Administration, and Microsoft Windows.

Equivalent to completion of twelfth grade and additional college courses or specialized training in computer programming, operating systems, network operations, or related fields. A bachelor's degree in a related field is highly desirable.

Special Requirements:

Must possess a valid driver's license at time of application and a valid California Driver's License by the time of appointment. The valid California Driver's License must be maintained throughout employment.

All County of Plumas employees are designated Disaster Service Workers through State law (California Government Code Section 3100-3109). Employment with Plumas County requires the affirmation of a loyalty oath to this effect. Employees are Required to complete all Disaster Service Work related training as assigned, and to return to work as ordered in the event of an emergency.

SAAS SYSTEMS ADMINISTRATOR

DEFINITION

Under general direction of the Director of Informational Technology to configure, maintain, and administer SAAS (software as a service) cloud-based computer systems used by numerous County departments; manage use of these applications for enhanced employee work performance.

DISTINGUISHING CHARACTERISTICS

This is a specialized classification position in the Informational Technology Department, which has responsibility for developing, coding, and debugging application programs for the County computer systems. The position also has responsibility for the development and maintenance of database applications, including but not limited to County's financial and personnel systems with access to confidential information.

Compliance management refers to an individual's ability to ensure that employees comply with the rules, procedures and policies related to SaaS applications. This skill is particularly important because it allows the Information Technology (IT) Department to maintain the security of the County's data. Compliance management requires SaaS professionals to communicate clearly about the expectations for the software, the creation of documents that explain the security policies and the organization of the SaaS software that Plumas County uses. This position will improve the County's use of software while also enhancing the security levels.

REPORTS TO

Director of Informational Technology

CLASSIFICATIONS DIRECTLY SUPERVISED

None

EXAMPLES OF DUTIES

- Administers County SAAS systems and assists related departments with personalized configuration, reporting (SSRS), training, documentation, and troubleshooting.
- Administers County internet facing presence (Webpage, Social Media, ADA compliance)
- Works with end users / departments to understand information needs and configures SAAS systems to meet those needs.
- Prepares thorough systems definitions, and documentation for new and existing systems.
- Performs complex work in the configuration, debugging, and enhancement of SAAS systems and programs.
- Administers County Office 365 tenant including, Email, SharePoint, Azure Active Directory, O365 security, and Office 365 applications.
- Administers county ERP and assists related departments with personalized configuration, reporting (SSRS), training, documentation, and troubleshooting.
- Installs and tests new computer hardware, software and operating systems.
- Maintain accurate records of automation related problems and solutions.
- Manage access to software applications to ensure security.
- Onboard and offload employees to the proper applications.
- Assist with developing and adhering to the department's fiscal budget.
- Optimize the SaaS Budget by identifying which software is most valuable to the County.
- Assists with desktop support, employee training and administration of SaaS applications.
- Acts as support member for system upgrades, integrations, and technical assistance as needed.
- Maintain systems to protect County data, employee confidential information, and other protective measures a necessary.
- Perform related duties as assigned by Director of Information Technology.

TYPICAL PHYSICAL REQUIREMENTS

Sit for extended periods; frequently stand and walk; normal manual dexterity and eye-hand coordination; some kneeling and stooping; physical ability to lift and move objects weighing up to 50 lbs.; corrected hearing and vision to normal range; verbal communication; use of office equipment including computers, telephones, calculators, copiers, and FAX.

TYPICAL WORKING CONDITIONS

Work is performed in an office environment; some exposure to dust and electrical energy; continuous contact with staff and the public.

DESIRABLE QUALIFICATIONS

Knowledge of:

- Compliance management to ensure County is compliant with rules, procedures, and policies related to SAAS applications.
- Maintain cybersecurity and ensure all employees know how to use and secure applications.
- Computerized information systems including hardware and software capabilities.
- Principles, methods, and procedures of application program development, testing, and maintenance.
- Coding languages to ensure SAAS custom applications are ready.
- Database application development languages used by County database software.
- Programming languages and available software packages.
- Recent developments, current literature, and sources of information regarding data processing and computer systems.
- Project development, management, and coordination.
- Development and conversion of applications and services to automated data processing.
- Configuration and documentation of general SAAS systems.
- ADA Compliance / Website Administration.
- Computer operating systems.

Ability to:

- Ability to communicate effectively with other employees and County leadership about budget, application usage and other issues related to SAAS applications.
- Interact effectively and collaborate with all types of people to ensure computer applications work effectively.
- Develop, implement, modify, and maintain application programs and database systems.
- Train users in the use of application programs and database applications.
- Analyze user data processing needs and develop programs and database applications to meet those needs.
- Develop documentation and user manuals for systems and programs.
- Prepare reports and correspondence.
- Effectively present ideas and recommendations orally and in writing.
- Effectively represent the programs, operations, and functions of the County Data Processing Division, with the public, other County staff, and other government agencies.
- Establish and maintain cooperative working relationships.
- Quickly and independently learn, document, and begin to train end users on new and existing SAAS systems.
- Analyze user information system needs and develop systems to meet those needs.
- Evaluate and prioritize projects under direction of the Information Technology Director
- Develop precise and clear documentation and user manuals.
- Communicate clearly and concisely, both orally and in writing.

Training and Experience:

Two (2) years of responsible experience in the field of computer programming, website development, or systems analysis, including experience in the field of SAAS systems administration, including O365 administration.

Specific knowledge of Office 365 Tenant Administration, Munis ERP, CivicPlus / CivicClerk, and Microsoft Windows.

Equivalent to completion of twelfth grade and additional college courses or specialized training in computer programming, operating systems, network operations, or related fields. Bachelor's degree related field is highly desirable.

Special Requirements:

Must possess a valid driver's license at time of application and a valid California Driver's License by the time of appointment. The valid California Driver's License must be maintained throughout employment.

All County of Plumas employees are designated Disaster Service Workers through State law (California Government Code Section 3100-3109). Employment with Plumas County requires the affirmation of a loyalty oath to this effect. Employees are Required to complete all Disaster Service Work related training as assigned, and to return to work as ordered in the event of an emergency.