Position Description

Requisition # 03020269
This contract appointment ends 1 year from the date of hire, with the possibility of extension or conversion to career.

Position Number: 02021628
Dept: ENT APPS & INFRASTRUCTURE SVCS - 061419
Position: PROFESSIONAL SERVICES SYSTEM ADMINISTRATOR /CLOUD SECURITY ANALYST

Approved Payroll Title Code: 0520
Approved Payroll Title: SYS ADM 4
Approved MSP Salary Grade: MSP25
Approved PSS Salary Grade: MSP25

POSITION DETAILS

This position will report to the Professional Services Supervisor, within the IET Professional Services Organization. Acts as a system administrator for campus infrastructure systems and client systems hosted within various cloud computing providers and at the campus Data Center locations. Will evaluate, architect, recommend and implement appropriate cloud hosted solutions to meet customer requirements.

Job Summary:

Provide expert level of technical support for AWS, Azure and on premise services. Provide support for Linux, Windows, and Firewall systems running enterprise critical systems that support the mission of the University. Analyze, plan, design, develop, test, implement, administer, secure, and troubleshoot servers and associated hardware, operating systems, and software.

Additionally, this position will be responsible for deploying the architected security solutions and guidelines in the AWS and Azure environments.

Campus Job Scope:

Department Specific Job Scope: System and Cloud Administration for Secure Research Computing Environment System and Cloud Administration

Positions Supervised: N/A
Essential Responsibilities:

30% CLOUD ADMINISTRATION
Provide expert-level administration for applications and environments using various cloud computing infrastructures, and client-hosted systems. Analyze, design, propose, implement and maintain cloud infrastructure in accordance with campus and security policies. Manage, provision and maintain identity systems within cloud providers. Deploy and manage cloud hosted networking, servers, storage and platform infrastructure. Work with systems administrators, operations staff, network administrators, database administrators, campus work groups, and/or vendors to analyze, resolve, or escalate technical systems issues.

30% SYSTEMS ADMINISTRATION
Install, upgrade, maintain and support various Windows and Linux Operating Systems (OS); provide technical support for infrastructure/client applications, i.e., AWS, Azure, Apache, IIS, Tomcat, ColdFusion, Oracle, Active Directory, MySQL, SQL Server, RDS, Rshiny, and Java. Perform systems monitoring/diagnosis/configuration/performance tuning to optimize effectiveness. Perform system logs analysis, use monitoring tools, manage user accounts, backup and recovery, and setup/testing/implementation of new applications. Perform routine patching and systems maintenance.

15% SCRIPTING/PROGRAMMING
Create/maintain scripts to automate administration and deployment of enterprise infrastructure and client hosted server environment, includes managing user accounts and systems resources. Develop and maintain scripts to assist administration of cloud infrastructure, server, application, and user accounts management. Develop and maintain scripts for programmatic system configuration changes. Design and Implement automated testing solutions to support continuous integration solutions.

15% SECURITY SUPPORT
Maintain systems for UC Davis CyberSafety compliance and NIST 800-171 and NIST 800-53 compliance. Install, upgrade, maintain and support various hardware and software firewalls. Provide administration/support for host and network security monitoring. Manage and maintain a SIEM.

10% COMMUNICATIONS/WORKING RELATIONSHIPS
Communicate in written and oral forms; develop and maintain good working relationships with other members of the Information and Educational Technology Professional Services unit, Information Security Office, other Information and Educational Technology departments, campus technical administrators, and vendors.
Communicate complex technical concepts to technical and non-technical audiences. Consult with system managers, application programmers, database administrators, and campus clients on application support, utilities, and operations system planning. Develop cost estimates for client projects.

Read LED screens for extended periods of time.

Sit for extended periods of time working at a computer terminal using a keyboard to enter and retrieve data.

Physical Demands:

Reach and work with equipment mounted in computer racks and be able to access and work with equipment that may be located anywhere from the bottom (floor level) to the top of 7-foot high racks.

Lift and move equipment weighing up to 50 pounds

Work occasional evenings/night, especially in response to emergencies. Vacation is restricted during busy times.

Travel to campus and off campus locations. Occasional travel is required.

Work Environment:

Must be routinely on-call as required and carry pager/cell phone.

UC Davis is a smoke and tobacco free campus effective January 1, 2014. Smoking, the use of smokeless tobacco products, and the use of unregulated nicotine products (e-cigarettes) will be strictly prohibited on any UC Davis owned or leased property, indoors and outdoors, including parking lots and residential space.

Background Check: Yes

QUALIFICATIONS

Minimum Qualifications:

Experience designing and deployment of cloud controls for infrastructure, platform, and applications (IaaS/SaaS/PaaS).

Experience incorporating security components in cloud, hybrid and on premises environments.

Experience with designing, implementing and maintaining services running on Amazon Web Services.
Experience with administering Linux and Windows servers in an enterprise environment.

Experience leading and participating in workgroups focusing on the technical aspects of implementing enterprise-wide distributed computing and computing security.

Experience generating broad guidelines and architectures that support development of enterprise-wide services or enhancements.

Experience to assess and implement computer security including the implementation of a security standard to both workstations and servers.

Experience performing needs analysis, system planning, design, procurement, testing, implementation, administration, troubleshooting, problem remediation, documentation, and capacity planning in an environment for both Enterprise and client applications with the ability to produce and present project proposals, project plans, service agreements, and status reports.

Preferred Qualifications for Selection:

Experience managing Amazon Web Services solutions including CloudFormation, EC2, VPC, S3, RDS, Security Groups, NACLs, System Manager, CloudWatch, CloudTrail, and Lambda.


Experience with one or more formal security frameworks (ie. PCI, HIPAA, FISMA etc.) Preference for experience with experience in NIST 800-171 and/or ITAR.

Experience implementing enterprise grade logging software (ie. Elk, Splunk, etc).

Skills to learn and understand business needs and apply IT solutions to meet business needs in a supportable manner, understanding the practical implications of the application of information technologies.

Interpersonal and written communication skills to communicate with tact to customers and technical levels at the University and to prepare
and present written and oral reports.

Skills to effectively collaborate with internal and external constituents in a manner to meet unit, department, project, campus, and organizational goals.

Skills to effectively manage activities and projects in a dynamic work environment, requiring frequent changes to work schedules, priorities, and scope.

Experience with system, hardware, and service administration of a complex distributed and integrated Linux and Windows environment including but not limited to configuration and maintenance of LDAP, NFS, Apache, Tomcat, MySQL, PHP, ColdFusion, IIS, SQL Server, Rshiny Active Directory and other applications and configuration and maintenance of multiple hardware platforms such as x86 systems, virtual hosts, SANs, network file systems, and firewalls. Experience installing, configuring, and performance tuning server platforms.

Basic programming experience with Perl, Powershell, shell scripts, Python, PHP, Ruby or similar languages.

Skills to implement serverless automation on platforms such as AWS Lambda or Azure Cloud Functions.

Experience with relational database systems such as Oracle, SQL Server, MySQL, PostgreSQL, and experience with SQL and database performance tuning.

Knowledge of campus infrastructure systems, including CAS, Shibboleth, DNS, and MIT's Kerberos, Exchange, Active Directory, and LDAP.

General knowledge of Identity and Access Management concepts.

A current Amazon Web Services Certification (AWS DevOps preferred)

A current Microsoft Azure Certification

A degree in Information Technology or a related field.

<table>
<thead>
<tr>
<th>Expectations</th>
</tr>
</thead>
</table>
Job Expectations

Read and demonstrate commitment and support of the UC Davis Principles of Community.

Excellent communication (oral, written, presentation, documentation) and interpersonal skills, using tact and diplomacy for interactions with others.

Independently follow projects through to successful completion with a high degree of quality.

Work independently and as a team to establish priorities and to exercise good judgment.

Excellent skills to establish priorities, organize tasks, and effective implementation of tasks in a demanding work environment.

Meet client expectations with an emphasis on quality, quantity and timeliness of work.

Convey a helpful and positive attitude to the public, campus departments and the various units in support of the department's client service environment.

Analytical skills to make to understand implications, and anticipate consequences.

Develop recommendations and alternative courses of action.

Integrate computer and network systems with existing campus infrastructure, including Active Directory, CAS, LDAP, and Kerberos services.

Accountability for the safekeeping of resources in the employee's care and custody and for following and implementing the cyber-safety guidelines.

Adhere to workplace safety practices, read information communicated about workplace safety, complete required safety training on time, report any workplace safety issues promptly to their supervisor or the designated safety coordinator.

Willingness to learn and apply new technology and willingness to develop skills to promote professional growth.

Provide informal training and mentoring to educate personnel in the use of products or services.
Be consistently punctual, reliable, and flexible in a dynamic work environment in which meetings and technical work are often at client sites with frequent changes in work priority, scope and schedules.