Infrastructure Connectivity Management and Engineering Student Learning Outcomes

	Knowledge	Student Learning Outcomes
K-46	Knowledge of Cloud and Cloud Services.	Describe cloud and cloud services technologies.
K-10	Knowledge of risk management, cybersecurity, and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Explain information security principles and fundamentals. Describe laws, regulations, and ethical behavior related to cybersecurity and privacy globally.
K-3	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy (e.g., PCI, PII, PHI, GDPR).	
K-4	Knowledge of cybersecurity and privacy principles.	
K-5	Knowledge of cyber threats and vulnerabilities.	Identify how to assess network vulnerabilities and attacks. Describe the operational implications to the organization of cybersecurity lapses.
K-6	Knowledge of specific operational impacts of cybersecurity lapses.	
K-42	Knowledge of systems concepts and methods.	Describe the network system components and their inter-relationships. Summarize the importance of asset management to the organization. Explain the components of storage infrastructure including subsystems and intelligent storage systems.
K-50	Knowledge of asset management and why it's important to the business.	
K-51	Knowledge of infrastructure data storage capabilities and storage clusters.	
K-23	Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA).	Distinguish between different enterprise network architecture and topologies - such as - Local Area Networks (LANs), Wide Area Networks (WANs).
K-36	Knowledge of the enterprise information technology (IT) architecture.	
K-21	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).	
K-14	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI]).	Explain the OSI model and different network protocols - such as - TCP and IP. Describe how to assess organization's existing infrastructure. Describe technology concepts for remote access.
K-9	Knowledge of how to assess existing infrastructure (LAN, WAN).	
K-15	Knowledge of remote access technology concepts.	
K-32	Knowledge of controls related to the use, processing, storage, and transmission of data.	Name and describe controls related to the use, processing, storage, and transmission of data. Name and describe types of data transmission and techniques of jamming and interference.
K-30	Knowledge of transmission types (e.g., Bluetooth, Radio Frequency Identification [RFID], Infrared Networking [IR], Wireless Fidelity [Wi-Fi]. paging, cellular, satellite dishes, Voice over Internet Protocol [VoIP]), and jamming techniques and interference techniques.	
K-31	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Install and configure DHCP, DNS, remote access, network security and directory services. Describe the current concepts of telecommunications. Explain the capabilities of different electronic communication systems and methods.
K-7	Knowledge of communication methods, principles, and concepts that support the network infrastructure.	
K-17	Knowledge of telecommunications concepts (e.g., will change all the time).	
K-19	Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).	
K-22	Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).	
K-24	Knowledge of Wi-Fi.	Describe how Wi-Fi works.
K-53	Knowledge of voice, video, and data transmission protocols.	Identify and use different media network transmission protocols.
K-54	Knowledge of IoT end devices and connectivity.	Describe commonly used IoT end devices and their connectivity.
K-1	Knowledge of computer networking concepts and protocols, and network security methodologies.	Identify and summarize techniques and protocols to secure network communication.
K-25	Knowledge of Voice over IP (VoIP).	Define and describe Voice over IP (VoIP).
K-8	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.	Describe the applications of different network hardware equipment in a business environment. Define and describe concepts of bandwidth management in a LAN/WAN networks.
K-12	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	
K-16	Knowledge of server administration and systems engineering theories, concepts, and methods.	Explain the concepts and methods of server administration.
K-20	Knowledge of network tools (e.g., ping, traceroute, nslookup).	Explain how different network commands and tools can be used to monitor and manage network performance.
K-28	Knowledge of network and systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools (NOC and SOC).	
K-33	Knowledge of performance tuning tools and techniques.	
K-34	Knowledge of server and client operating systems.	Recognize common issues with different operating systems and server administration.
K-35	Knowledge of systems administration concepts.	
K-37	Knowledge of the type and frequency of routine hardware maintenance (e.g., Linux/Unix OS, Windows Server OS).	Summarize the organization's schedule and procedures for routine hardware maintenance. List and describe different file systems and extensions including network storage, servers, and file transfer protocols.
K-38	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]) including network storage and servers.	
K-39	Knowledge of virtualization technologies and virtual machine development and maintenance.	Outline the concepts of network virtualization, including virtual machine development and maintenance.
K-40	Knowledge of information technology (IT) user security policies (e.g., account creation, password rules, access control).	Describe the organization's user security policies.

K-41	Knowledge of system administration, network, and operating system hardening techniques.	Describe how to administer a network operating system including hardening techniques. Explain the organization's system/server diagnostic tools and fault identification techniques.
K-43	Knowledge of system/server diagnostic tools and fault identification techniques.	
K-44	Knowledge of operating system command-line tools.	List the operating system command-line tools. Describe the principles and methods used to integrate network system components.
K-45	Knowledge of principles and methods for integrating system components including network storage and servers.	
K-48	Knowledge of network backup and recovery procedures.	Describe the organization's network backup and restoration process.
K-55	Knowledge of metrics, how they are developed in general, their purpose, and why they are used.	Recognize and understand the latest tools for network traffic metrics and system performance.
K-13	Knowledge of measures or indicators of system performance and availability.	
K-26	Knowledge of the common attack vectors on the network layer.	List common attack vectors on the network layer. Describe concepts of network security architecture including Network Security Devices, Protocols and Topologies.
K-27	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	
K-18	Knowledge of Virtual Private Network (VPN) security.	Recognize the administration of Virtual Private Network (VPN).
K-29	Knowledge of concepts of certificates, key management, and usage.	Explain the concepts of Key Management and Certificate Lifecycles. Identify and describe various information technology security principles and methods.
K-11	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	
K-49	Knowledge of patch network vulnerabilities to ensure that information is safeguarded against outside parties.	Explain Network Vulnerability Assessment and Data Security at physical and cloud locations.
K-52	Knowledge of risks associated with storing various types of data in different physical locations.	
K-2	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Explain the importance of Control Access to mitigate risk and vulnerabilities in all networks environment.
K-47	Knowledge of script automation and application programming interfaces.	Describe the importance of APIs and use of script automation in network environment.
Cloud K-1	Knowledge of the differences or similarities between private, public, and hybrid cloud implementations.	Compare and contrast public, private, and hybrid cloud. Recognize different XaaS tools and technologies models.
Cloud K-2	Knowledge of the difference or similarities between Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models.	
Cloud K-3	Awareness of framework concepts, their selection, and use.	Generalize the selection and use of cloud framework concepts.
Cloud K-4	Awareness of the pros or cons behind using frameworks.	
Cloud K-5	Knowledge of the term benchmarks and the reasons for their use.	Describe benchmarks as performance metrics. Describe how to design resilience into projects and components of an organization.
Cloud K-6	Knowledge of the term resilience and how resilience can be designed into a project, program, infrastructure, or organization.	
Cloud K-7	Knowledge of the concept of service level agreement (SLA), why they are used, when they are used, and its application within cloud implementations.	Describe how, why, and when Service Level Agreements (SLA) are implemented in a cloud environment. Define and explain the applicability of high availability service levels.
Cloud K-25	Knowledge of high availability service levels (SLA).	
Cloud K-8	Knowledge of who owns or should own the data/information in a cloud implementation.	Explain data ownership in a cloud implementation. Describe management, operational, security, and privacy challenges when considering cloud implementation.
Cloud K-9	Knowledge of the key management, operational, security, and/or privacy challenges potentially faced when considering or implementing a cloud capability.	
Cloud K-10	Knowledge of the different organizational roles needed as one plans for cloud implementation or manages an existing cloud capability.	Describe organizational roles needed for a planned cloud implementation. Describe incident response challenges in a cloud implementation.
Cloud K-11	Knowledge of the incident response challenges potentially faced within a cloud implementation.	
Cloud K-13	Knowledge of cloud network storage.	Describe different cloud storage systems including local, network and object-based.
Cloud K-14	Knowledge of cloud object-based storage.	
Cloud K-15	Knowledge of cloud local system storage.	
Cloud K-16	Knowledge of the different cloud computing database types (RDS).	Differentiate and describe scalability of cloud based databases such as RDS,SQL and Non-SQL. Describe how to implement a cloud database solution that meets the requirements. Describe best practices in database fail-over processes.
Cloud K-17	Knowledge of how to scale a cloud database.	
Cloud K-18	Knowledge of cloud database fail-over best practices.	
Cloud K-19	Knowledge of the differences between SQL and Non-SQL databases.	
Cloud K-32	Knowledge (not skill) in preparing and deploying a cloud database solution that meets application requirements.	
Cloud K-20	Knowledge of cloud IAM (Identity and Access Management).	Summarize and explain the life cycle of users with Identity and Access Management.
Cloud K-21	Knowledge of cloud IAM (Identity and Access Management) users, groups, roles, and policies.	
Cloud K-22	Knowledge of cloud computing shared security responsibility model.	Describe the cloud computing shared security responsibility model.
Cloud K-23	Knowledge of cloud regions.	Explain cloud regions and availability zones in cloud infrastructure.
Cloud K-24	Knowledge of cloud availability zone.	
Cloud K-26	Knowledge of recovery time objective (RTO).	Compare and contrast Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
Cloud K-27	Knowledge of recovery point objective (RPO).	
Cloud K-28	Knowledge of high availability factors (fault-tolerance, recoverability, and scalability).	Explain high availability factors in a cloud environment.

Cloud K-12	Knowledge of web services technologies.	Describe and explain the use of web services technologies tools such as microservices and containerization.
Cloud K-29	Knowledge of microservices and containerization (e.g., Kubernetes and Docker).	
Cloud K-30	Knowledge of auto scaling and load balancing.	Describe capabilities of cloud auto scaling and load balancing. Describe the difference between cloud technologies and traditional networks.
Cloud K-31	Knowledge of the differences between cloud vs. on-premises.	
	Skills	**Student Learning Outcomes**
S-4	Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers and switches.	Install network components and perform configuration. Implement a basic network security configuration and recovery plan.
S-9	Skill in testing network infrastructure contingency and recovery plans.	
S-2	Skill in establishing a routing schema.	Apply the TCP/IP concepts to addressing schema and subnetting.
S-10	Skill in applying various subnet techniques (e.g., CIDR).	
S-11	Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).	Demonstrate skills in installing and configuring network hardware, software and cable, including firewalls and other devices. Demonstrate skill in diagnosing network connectivity problems.
S-12	Skill in configuring and basic optimizing software.	
S-13	Skill in diagnosing connectivity problems.	
S-14	Skill in maintaining directory services (e.g., Microsoft Active Directory, LDAP, etc.).	Manage file system and directory services operations. Build and adapt different types of virtual machines. Build apps using containerized software tools.
S-15	Skill in using virtual machines (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).	
S-17	Skills in using microservices and containers (e.g., Docker, Kubernetes, ECS) and understanding monitoring dashboards.	
S-18	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).	Apply basic software security measures to protect network devices. Perform troubleshooting services including software upgrade/downgrade and installation of appropriate network devices.
S-20	Skill in conducting system/server management and maintenance.	
S-22	Skill in troubleshooting failed system components (i.e., servers).	
S-24	Skill in installing system and component upgrades (i.e., servers, appliances, network devices).	
S-25	Skill in monitoring and optimizing basic system/server performance.	Create and maintain an effective network performance baseline by monitoring and troubleshooting network performance.
S-23	Skill in identifying system/server performance, availability, capacity, or configuration problems.	
S-21	Skill in correcting physical and technical problems that impact system/server performance.	
S-26	Skill in recovering failed systems/servers (e.g., recovery software, failover clusters, replication, etc.).	Perform the recovery process for a failed system or server. Create, administer, and maintain user accounts and groups in a network environment.
S-27	Skill in operating system administration (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).	
S-1	Skill in analyzing network traffic capacity and performance characteristics.	Utilize the latest tools to analyze network traffic and identify patterns to improve performance.
S-5	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).	
S-6	Skill in securing network communications (e.g., logical).	Take appropriate actions to mitigate vulnerability and risk from potential network attacks.
S-7	Skill in protecting a network against malware (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	
S-8	Skill in basic configuring and utilizing network protection components (e.g., firewalls, VPNs, network intrusion detection systems).	
S-3	Skill in implementing, maintaining established network security practices.	Apply established practices to secure a network.
S-19	Skill in interfacing with customers.	Demonstrate effective interactions with customers.
Cloud S-1	Skill in identifying and distinguishing private, public, and hybrid cloud implementations.	Discuss public, private, and hybrid cloud technologies. Explain different XaaS tools and technologies models. Operate and manage cloud technologies. Perform different functional and non-functional cloud tests to ensure business requirements. Summarize and document cloud testing results against developed criteria.
Cloud S-2	Skill in identifying and distinguishing Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models.	
S-16	Skill in using cloud (e.g., Amazon Elastic Compute Cloud).	
Cloud S-3	Skill in executing test cases for identified functional or non-functional requirements.	
Cloud S-4	Skill in documenting results of executed test cases showing whether according to developed success criteria the test case passes, fails, or partially passes.	
Cloud S-5	Skill in documenting and determining root cause failure(s) for items that failed or partially passed.	
Cloud S-8	Skill in producing virtual machines from a cloud image.	Demonstrate setting up virtual machine(s) using cloud technologies.
Cloud S-9	Skill in producing virtual machines within a cloud region.	
Cloud S-10	Skill in demonstrating how to customize virtual networks with IP address range, subnets, routing tables and gateways.	Prepare customized virtual machine(s) based on different network topologies. Troubleshoot issues with virtual machine(s).
Cloud S-11	Skill in analyzing and troubleshooting cloud virtual networks.	
Cloud S-12	Skill in preparing and deploying virtual machines in a virtual network (private or public subnet).	
Cloud S-15	Skill in applying permissions from the IAM (Identity and Access Management).	Demonstrate and apply the life cycle of users and groups with Identity and Access Management.
Cloud S-16	Skill in applying permissions for IAM (Identity and Access Management) group(s).	
Cloud S-17	Skill in applying permissions for IAM (Identity and Access Management) user(s).	
Cloud S-18	Skill in preparing and deploying a cloud high availability and business continuity solution.	Develop and implement a cloud backup and business continuity disaster recovery plan.
Cloud S-19	Skill in deploying a containerized application.	Deploy a distributed system by applying containerization tools.
Cloud S-20	Skill in analyzing and troubleshooting containers.	
Cloud S-21	Skill in implementing auto scaling and load balancing.	Perform auto scaling and load balancing on cloud servers.
Cloud S-13	Skill in deploying cloud storage technologies with the assistance of a senior technician.	Deploy different cloud storage systems with assistance from a senior technician. Analyze and troubleshoot different cloud storage systems.
Cloud S-14	Skill in analyzing and troubleshooting different cloud storage technologies.	

Cloud S-22	Skill in using management tools like Chef, Puppet, etc.	Utilize management tools for improving infrastructure automation.
Cloud S-6	Skill in preparing written reports.	Develop effective written reports and presentations to deliver information to an appropriate audience.
Cloud S-7	Skill in preparing presentations.	
	Abilities	**Student Learning Outcomes**
A-6	Ability to operate different electronic communication systems and methods (e.g., e-mail, VoIP, IM, web forums, Direct Video Broadcasts).	Apply techniques and protocols to data communication network systems.
A-1	Ability to install network equipment including routers, switches, servers, transmission media, and related hardware.	Integrate LAN/WAN network connectivity by installing network hardware, software and cabling.
A-4	Ability to operate the organization's LAN/WAN pathways.	Operate the organization's LAN/WAN pathways.
A-10	Ability to apply an organization's goals and objectives to maintain architecture.	Ensure network architecture aligns with organization's goals and objectives. Demonstrate the use of OS command line tools.
A-3	Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).	
A-9	Ability to interpret and clarify incidents, problems, and events submitted in the trouble ticketing system.	Assess and troubleshoot issues submitted to the organization's ticketing system.
A-2	Ability to operate common network tools (e.g., ping, traceroute, nslookup).	Measure network system traffic by using network tools to improve performance.
A-5	Ability to monitor measures or indicators of system performance and availability.	
A-7	Ability to monitor traffic flows across the network.	
A-8	Ability to recognize and escalate the information collected by network tools (e.g., nslookup, ping, and traceroute).	Analyze the data collected from network tools to identify problems.
A-14	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Facilitate organization's cybersecurity, privacy, and security controls for the network environment.
A-15	Ability to maintain automated security control assessments.	
A-11	Ability to update, and/or maintain standard operating procedures (SOPs).	Maintain the organization's standard operating procedures (SOPs) and update as needed.
Cloud A-1	Ability to work within a project team.	Demonstrate effective collaboration skills to work with a team to achieve project goals.
A-12	Ability to collaborate effectively with others.	
Cloud A-2	Ability to communicate effectively (written and oral) within and among team members and associated stakeholders (i.e., different audiences and organizational levels). This includes communicating complex technical issues and business implications.	Demonstrate effective communication skills (both oral and written) when working with team members and stakeholders. Effectively communicate technical jargon in simple terms to team members and stakeholders. Demonstrate effective listening skills. Analyze and interpret input to determine implicit and explicit customer requirements.
Cloud A-6	Ability to translate technical language into lay terminology when needed.	
Cloud A-8	Ability to listen and understand what people say.	
Cloud A-5	Ability to analyze and interpret customer input for expressed and implied requirements.	
A-13	Ability to function effectively in a dynamic, fast-paced environment.	Demonstrate the ability to successfully perform job functions in a fast-paced and dynamic work environment.
Cloud A-3	Ability to work under stress.	Demonstrate the ability to successfully perform job functions in stressful situations.
Cloud A-4	Ability to problem solve.	Demonstrate the ability to understand details, prioritize items, and use available information to solve problems.
Cloud A-9	Ability to recognize and understand details.	
Cloud A-10	Ability to order and arrange items.	
Cloud A-7	Ability to read and interpret technical documents, diagrams, and decision trees.	Analyze and interpret technical documents and diagrams.
Cloud A-11	Ability to create appropriate presentation visuals for technical material.	Develop presentation visuals to deliver technical information to an appropriate