IT SKILL STANDARDS 2020 AND BEYOND

“Technical Support”

Job Cluster

Acknowledgements

The development and publication of these skill standards has been a joint and collaborative effort between business and industry representatives and the education community. We are grateful to the industry personnel who participated in the development and validation process. Industry subject matter experts, technical executives, supervisors and technicians donated their time and effort to assure the relevancy of the standards 12 to 36 months into the future.

We gratefully acknowledge funding from the National Science Foundation and the leadership by the team on the IT Skill Standards 2020 and Beyond grant, based at Collin College.

Our leaders are strategically divided into Central, Western, and Eastern teams.

Central

Dr. Ann Beheler, Principal Investigator

Christina Titus, Program Director

Deborah Roberts, Co-Principal Investigator

Helen Sullivan, Senior Staff

West Coast

Terryll Bailey, Co-Principal Investigator

Dr. Suzanne Ames, Co-Principal Investigator

East Coast

Peter Maritato, Co-Principal Investigator

Gordon Snyder, Senior Staff

This material is based upon work supported by the National Science Foundation under Grant No. 1838535. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

itskillstandards.org

Technical Support

The definition for Technical Support as developed by approximately 100 Thought Leaders (mostly Chief Technology Officers and Chief Information Officers) through three meetings and follow-up surveys to gain consensus is:

Technical Support refers to services that entities provide to users of technology products or services. In general, technical support provides help regarding specific problems with a software, hardware or network product or service. In some organizations it may include training. This definition was adapted from Wikipedia with input from national IT Thought Leaders.

This packet includes…

Job skills as developed by subject matter experts (SMEs) via multiple synchronous meetings (Page 5).

The tasks, knowledge, skills and abilities (KSAs) were developed with a focus 12 to 36 months in the future for an entry-level employee working in that specific cluster.

More specific definitions can be found within the KSA list.

The average was calculated from the subject matter expert votes.

- A vote of "4" indicated the item must be covered in the curriculum.
- A vote of "3" indicated the item should be covered in the curriculum.
- A vote of "2" indicated that it would be nice for the item to be covered in the curriculum.
- A vote of "1" indicated the item should not be covered in the curriculum.

Employability Skills as developed by SMEs via multiple synchronous meetings (Page 8).

Employability competencies are essential for every IT job and are based on what the work requires. SMEs were offered three clearly-defined “levels of proficiency” for each employability skill. The proficiency scale is defined as Level 1 – basic: Level 2- intermediate; and Level 3 - advanced. The levels are cumulative, so a “Level 3” assumes the employee can perform all characteristics of “Level 1” and “Level 2.”

For each employability skill, SMEs selected the competency level that best aligned with what would be expected from an entry-level worker for the job cluster in question.

Key Performance Indicators (KPIs) as developed by SMEs (Page 10).

Key Performance Indicators answer the question, “How do we know when a task is performed well?”

A search was performed to locate validated/verified KPIs for technician level work in IT fields. Sources included the Texas Skill Standards System, National Skill Standards Board, National Institute of Standards and Technology and other sources. The identified KPIs were then cross-referenced to the tasks for the ITSS 2020 job clusters. They were reviewed and revised by a group of the same subject matter experts who developed the tasks and KSAs for the cluster in a structured, facilitated verification session.

Student Learning Outcomes (SLOs) as identified by educators attending the KSA meetings (Page 11).

The SLOs are for use in the creation of curriculum to help define what the students will know and be able to demonstrate. Each of these SLOs can be observed, measured, and demonstrated.

Degree Expectations as identified by educators (Page 14).

A pool of 36 community college and four-year university faculty members from across the country were asked to categorize each knowledge, skill, ability, and task below. The question posed to them: would these KSA+Ts be reasonably included in a two-year AAS program, a four-year Bachelor's program, both, or neither? These results provide another tool for educators to use in assessing how to best incorporate each knowledge, skill, ability, and task.

Technical Support Tasks and KSAs

		Avg
Tasks SPECIFIC THINGS an entry level person would BE EXPECTED TO PERFORM on the job WITH LITTLE SUPERVISION.		
Install, Configure, Update, Maintain		
T-1	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	3.3
T-2	Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.	3.3
T-3	Manage changes/updates for both internal and external customers when policies and procedures change.	3.0
T-4	Maintain computer hardware.	2.8
T-5	Provide technical support for software maintenance or use.	3.6
T-6	Troubleshoot system hardware and software.	3.4
T-7	Diagnose and resolve customer-reported system incidents, problems, and events.	3.3
T-8	Identify, test, and implement solutions to computer hardware and software problems or escalate if required.	3.5
T-9	Test software performance in relation to troubleshooting.	2.8
T-10	Test computer hardware performance in relation to troubleshooting.	2.6
T-11	Collaborate with others to resolve information technology issues.	3.3
T-12	Identify and escalate issues to improve computer or information systems.	3.2
T-13	Escalate computer hardware and software problems according to organization policies.	3.3
T-14	Monitor and report client-level computer system performance.	3.3
T-15	Monitor computer system performance to ensure proper operation.	3.1
T-16	Assess or monitor system for cyberattacks.	3.3
T-17	Responds to crises/security incidents following SOPs.	3.3
T-18	Learn continuously about emerging industry or technology trends (e.g., machine learning and AI).	3.2
T-19	Administer accounts, network rights, and access to systems and equipment.	3.5
T-20	Perform asset management/inventory of information technology (IT) resources.	2.8
T-21	Maintain incident tracking and solution database.	2.8
T-22	Effectively document operational activities and enter results into the knowledge base and/or ticketing systems.	3.3
Knowledge Knowledge focuses on the understanding of concepts. It is theoretical. An individual may have an understanding of a topic or tool or some textbook knowledge of it but have no experience applying it. For example, someone might have read hundreds of articles on health and nutrition, many of them in scientific journals, but that doesn't make that person qualified to dispense advice on nutrition.		
K-1	Knowledge of the basic operation of computers.	3.9
K-2	Knowledge of computer networking concepts and protocols and network security methodologies.	3.6
K-3	Knowledge of operating environments, organizational software and applications.	3.3
K-4	Knowledge of practices of internal, external, and global customers (as applicable).	2.8
K-5	Knowledge of internal organizational communication processes.	3.1
K-6	Knowledge of customer support processes and practices.	3.7
K-7	Knowledge of technical support operations, issues, and constraints.	3.4
K-8	Knowledge of business issues regarding software licensing.	3.0
K-9	Knowledge of interrelation between different organizational groups.	2.5
K-10	Knowledge of organization chart and roles/responsibilities of company personnel/departments.	2.7
K-11	Knowledge of preventative maintenance procedures and processes.	3.3
K-12	Knowledge of applicable backup and restoration procedures.	3.5
K-13	Knowledge of system monitoring and diagnostic tools and processes.	3.5
K-14	Awareness of the components of the risk management process (e.g., methods for assessing and mitigating risk).	3.0
K-15	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	3.0
K-16	Knowledge of cybersecurity and privacy principles.	3.8

K-17	Knowledge of cyber threats and vulnerabilities.	3.3
K-18	Knowledge of specific operational impacts of cybersecurity lapses.	3.2
K-19	Knowledge of measures or indicators of system performance and availability.	3.0
K-20	Knowledge of systems administration concepts.	3.1
K-21	Knowledge of physical computer components and architectures, including the functions of various components and peripherals.	3.3
K-22	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).	3.1
K-23	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).	3.1
K-24	Knowledge of Cloud-based technologies and concepts (e.g., IAAS, SAAS, PAAS, file/sync/share).	3.6
K-25	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	3.4
K-26	Knowledge of industry best practices for service desk (e.g., machine learning and AI).	3.1
K-27	Knowledge of organizational security policies.	3.4
K-28	Knowledge of remote access processes, tools, and capabilities related to customer support.	3.6
K-29	Knowledge of Personally Identifiable Information (PII) data security standards.	3.3
K-30	Knowledge of Payment Card Industry (PCI) data security standards at an awareness level.	2.9
K-31	Knowledge of Personal Health Information (PHI) data security standards.	3.1
K-32	Knowledge of an organization's information classification program and procedures for information compromise.	2.8
K-33	Knowledge of the operations and processes for incident, problem, and event management including escalation as needed.	3.3
K-34	Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.	3.3
K-35	Knowledge of procedures used for documenting and querying reported incidents, problems, and events.	3.0
K-36	Knowledge of successful capabilities to identify the solutions to less common and more complex system problems.	3.1
K-37	Knowledge of principles and processes for providing customer and personal services. This includes customer needs assessment, knowledge assessment, meeting quality standards for services, and evaluation of customer satisfaction.	2.8
K-38	Knowledge of the structure and content of the English language including the meaning and spelling of words, rules of composition, and grammar.	3.3
K-39	Knowledge of troubleshooting methods.	3.6
K-40	Knowledge of change control procedures.	3.3
K-41	Knowledge of documentation processes and procedures.	3.1
K-42	Knowledge of technical presentation tools.	2.6
K-43	Knowledge of continuous quality improvement.	2.8
K-44	Knowledge of VOIP telecommunication systems, both cloud-based and on premise, as well as the OSI model and common networking protocols.	2.8
K-45	Knowledge of what is cloud-based and what is on premises as well as the different support models for each.	3.4
K-46	Knowledge of when to escalate to vendor or providers and how to monitor progress through solution.	3.2
K-47	Knowledge of cybersecurity trends and effect of changes due to cybersecurity event.	3.0
K-48	Knowledge of change management approaches and communication.	2.9
K-49	Knowledge of security threats.	3.6
K-50	Knowledge of professional services automation and management (e.g. security patches that are automatically deployed).	3.0
K-51	Knowledge of case management tools, processes, and procedures.	3.1
K-52	Knowledge of crisis management processes and procedures.	2.9

Skills The capabilities or proficiencies developed through training or hands-on experience. Skills are the practical application of theoretical knowledge. Someone can take a course to gain knowledge of concepts without developing the skills to apply those concepts. Development of skills requires hands-on application of the concepts.		
S-1	Skill in identifying possible causes of degradation of system performance or availability as well as skill in initiating actions needed to mitigate this degradation.	3.3
S-2	Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system.	3.3
S-3	Skill in conducting research for troubleshooting novel client-level problems.	3.1
S-4	Skill in configuring and validating network workstations and peripherals in accordance with approved standards and/or specifications.	3.3
S-5	Skill in incident response for on premises or cloud service models.	3.3
S-6	Skill in communicating with others.	3.7
S-7	Skill in listening to others, not interrupting, and asking good questions.	3.7
S-8	Skill in recognizing a problem and figuring out the best way to solve it.	3.5
S-9	Skill in thinking about the pros and cons of different ways to solve a problem.	3.4
S-10	Skill in writing for communicating with co-workers or customers.	3.2
S-11	Skill in reading work-related technical information.	3.5
S-12	Skill in monitoring workload, managing time, and prioritizing requests.	3.4
S-13	Skill in adapting to and implementing change as a result of cybersecurity incident or AI directive.	3.3
S-14	Skill in applying techniques for handling unhappy customers professionally.	3.7
S-15	Skill in communicating with a customer at a level they can comprehend.	3.7
Abilities Abilities have historically been used to describe the innate traits or talents that a person brings to a task or situation. Many people can learn to negotiate competently by acquiring knowledge about it and practicing the skills it requires. A few are brilliant negotiators because they have the innate ability to persuade. In reality, abilities may be included under skills or may be separated out.		
A-1	Ability to analyze and interpret customer input for expressed and implied issues.	3.4
A-2	Ability to accurately define incidents, problems, and events in the trouble ticketing system.	3.4
A-3	Ability to follow, develop, update, and/or maintain standard operating procedures (SOPs).	2.9
A-4	Ability to find solutions to less common and more complex system problems including escalating problems when needed.	3.0
A-5	Ability to translate technical language into lay terminology when needed.	3.2
A-6	Ability to communicate verbally, appropriately for different audiences and organizational levels.	3.2
A-7	Ability to communicate complex technical issues and business implications.	2.9
A-8	Ability to read and interpret technical documents, diagrams, and decision trees.	3.4
A-9	Ability to record data in knowledge bases using proper keywords.	3.5
A-10	Ability to listen and understand what people say.	3.8
A-11	Ability to recognize and understand details.	3.7
A-12	Ability to speak clearly.	3.7
A-13	Ability to make order out of ambiguity.	3.5
A-14	Ability to use rules to solve problems.	3.3
A-15	Ability to communicate by writing.	3.6
A-16	Ability to create appropriate presentation visuals for technical material.	2.5
A-17	Ability to adjust to changing technology.	3.5

Technical Support Employability Skills

Workplace Professionalism & Work Ethics	Level 1 - Employee learns expectations of workplace environment (professional behavior and ethics) and adheres to practices with some guidance. Level 2 - Employee exhibits sound professionalism, judgment, and integrity and accepts responsibility for own behavior. Employee exhibits these qualities without guidance but occasionally refers to policies as needed.
Written Communication	Level 1 - Employee understands written instructions and executes tasks with guidance and feedback from supervisor. Employee clearly communicates concepts in writing. Level 2 - Employee comprehends and executes written instructions with minimal guidance. Employee composes well-organized written documents.
Oral Communication	Level 1 - Employee understands oral instructions and executes tasks with guidance and feedback from supervisor. Employee communicates concepts orally while clarifying for meaning. Employee develops listening skills. Level 2 - Employee comprehends and executes oral instructions with minimal guidance and exhibits good listening skills. Employee clarifies for meaning without needing prompting from supervisor.
Teamwork	Level 1 - With guidance and feedback from supervisor, employee obeys team rules and understands team member roles. Employee actively participates in team activities, volunteers for special tasks, and establishes rapport with co-workers. Level 2 - Employee demonstrates commitment, enthusiasm and supports team members. Employee follows up on assigned tasks and leads by example.
Problem Solving & Critical Thinking	Level 1 - Employee identifies the problem and relevant facts and principles with guidance and feedback from supervisor. Employee summarizes existing ideas and demonstrates creative thinking process while problem solving. Level 2 - With minimal supervision, employee analyzes underlying causes, considers risks and implications and uses logic to draw conclusions. Employee applies rules and principles to processes and recommends solutions.
Organization and Planning	Level 1 - Employee prepares schedule for self, monitors and adjusts task sequence, and analyzes work assignments with guidance from supervisor. Level 2 - Employee manages timelines and recommends timeline adjustments. Employee escalates timeline-impacting issues as appropriate.
Adaptability and Flexibility	Level 1 - With guidance and feedback from supervisor, employee is able to adjust ways of doing work based on changing dynamics. Working under pressure is difficult, but employee makes it through the project with guidance and oversight. Level 2 - Employee makes inquiries of co-workers regarding possible changes needed in ways of doing work and adapts accordingly. Observes co-workers increasing work productivity under pressure and follows their lead.
Initiative	Level 1 - Employee finishes a step in a project and waits for direction before going on to the next step. Level 2 - Employee finishes multiple steps in a project and appropriately begins working on the next step without being asked.
Accuracy	Level 1 - Employee makes mistakes routinely but is committed to learning to adjust work habits to prevent them in the future. Level 2 - Employee occasionally makes mistakes but quickly makes adjustments to work habits to avoid making the same mistake twice.
Cultural Competence	Level 1 - Employee is inexperienced with working with diverse teams. With support and guidance and getting to know team members, employee develops working relationships. Level 2 - Employee is committed to working with diverse teams but struggles when differences arise. Employee identifies those challenges and works with colleagues to find ways to work effectively. Level 3: Easily works with diverse teams to achieve collective goals. Demonstrates empathy and respect for all colleagues leading to positive working relationships throughout the organization.

Self and Career Development	Level 1 - Employee requires feedback and direction from supervisor regarding improvement needed in professional and technical skills. Employee follows through with skills development with monitoring by supervisor. Level 2 - Employee builds upon self-assessment experience and can develop a professional and technical skills improvement plan in conjunction with supervisor. Employee completes development plan without prompting from supervisor.

Technical Support Key Performance Indicators

For the entry-level employee, all tasks are typically done under supervision for as much as the first year and then with some independence with verification after the employee has more experience. All tasks are done according to company guidelines.

	Task	Key Performance Indicators
Install, Configure, Update, Maintain		
T-1	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	Current hardware, software and system documentation are obtained and evaluated. System hardware and peripherals are installed, configured and maintained according to specifications. System and peripherals are tested for functionality and performance. Operating and application software are installed, configured and upgraded according to specifications. Maintenance includes appropriate follow-up action according to company policy. Changes are documented and distributed in accordance with company policy.
T-2	Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.	
T-3	Manage changes/updates for both internal and external customers when policies and procedures change.	
T-4	Maintain computer hardware.	
T-5	Provide technical support for software maintenance or use.	
Troubleshoot and Support		
T-6	Troubleshoot system hardware and software.	Users/customers are serviced in timely manner. Customer input is gathered and analyzed. Relationships are managed so that users/customers are satisfied with the level of service. Problems are correctly identified and causes are isolated. Solutions are thoroughly researched, using existing knowledge base. Solutions are tested in a complete and realistic manner. Test scenarios are representative of actual use and environment. Resolutions are documented to the appropriate level of detail in accordance with company policy.
T-7	Diagnose and resolve customer-reported system incidents, problems, and events.	
T-8	Identify, test and implement solutions to computer hardware and software problems or escalate if required.	
T-9	Test software performance in relation to troubleshooting.	
T-10	Test computer hardware performance in relation to troubleshooting.	
T-11	Collaborate with others to resolve information technology issues.	
T-12	Identify and escalate issues to improve computer or information systems.	
T-13	Escalate computer hardware and software problems according to organization policies.	
Monitor		
T-14	Monitor and report client-level computer system performance.	System performance is monitored and reported according to procedures. Disruptions, outages, security violations and attacks of network services are monitored, recognized and reported in a timely manner, in accordance with company policies and procedures.
T-15	Monitor computer system performance to ensure proper operation.	
T-16	Assess or monitor system for cyberattacks.	
T-17	Responds to crises/security incidents following SOPs.	
Research and Evaluation		
T-18	Learn continuously about emerging industry or technology trends (e.g., machine learning and AI).	Initiative is demonstrated regarding pursuit of research and/or training opportunities on emerging industry or technology trends.
Administration		
T-19	Administer accounts, network rights, and access to systems and equipment.	Accounts are set up following standard operating procedures. Incidents are documented via the company incident tracking system and procedures. Documentation is clear and accurate and follows organization format and procedures. Assets are tracked and documented in accordance with company policy.
T-20	Perform asset management/inventory of information technology (IT) resources.	
T-21	Maintain incident tracking and solution database.	
T-22	Effectively document operational activities and enter results into the knowledge base and/or ticketing systems.	

Technical Support Student Learning Outcomes		
	Knowledge	**Student Learning Outcomes**
K-9	Knowledge of interrelation between different organizational groups.	Describe a company's organizational structural, group roles and responsibilities, and internal and external communication processes.
K-10	Knowledge of organizational chart and roles/responsibilities of company personnel/departments.	
K-32	Knowledge of an organization's information classification program and procedures for information compromise.	
K-5	Knowledge of internal organizational communication processes.	
K-35	Knowledge of procedures used for documenting and querying reported incidents, problems, and events.	Explain a company's business process for systems documentation. Discuss business processes and issues for IT professionals including privacy laws, software licensing, ethical and professional behavior.
K-41	Knowledge of documentation processes and procedures.	
K-8	Knowledge of business issues regarding software licensing.	
K-2	Knowledge of computer networking concepts and protocols, and network security methodologies.	Explain the OSI model as it applies to various network environments. Identify and summarize techniques to secure network communication. Demonstrate the use of operating system commands to manipulate files and directories and perform systems software troubleshooting. Explain various terminologies and technologies related to cloud-based systems. Differentiate between public, private, and hybrid cloud-based environments. Describe the Voice over Internet Protocol (VoIP) telecommunications systems within the networking protocols.
K-20	Knowledge of systems administration concepts.	
K-28	Knowledge of remote access processes, tools, and capabilities related to customer support.	
K-19	Knowledge of measures or indicators of system performance and availability.	
K-24	Knowledge of cloud-based technologies and concepts (e.g., IAAS, SAAS, PAAS, file/sync/share).	
K-44	Knowledge of VOIP telecommunication systems, both cloud-based and on premise, as well as the OSI model and common networking protocols.	
K-45	Knowledge of what is cloud-based and what is on premises as well as the different support models for each.	
K-21	Knowledge of physical computer components and architectures, including the functions of various components and peripherals .	Identify and resolve common hardware faults and failures. Describe how to install, configure, diagnose, and perform preventive maintenance on different hardware devices. Identify the components of integrating the TCP/IP protocol into the networking environment. Discuss how to identify issues with software installation, configuration, permissions, and licensing restrictions. Describe how to assemble commonly required components in standard desktop/laptop computers.
K-22	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).	
K-34	Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.	
K-1	Knowledge of the basic operation of computers.	
K-11	Knowledge of preventative maintenance procedures and processes.	
K-12	Knowledge of applicable backup and restoration procedures.	Discuss the organization's backup and restoration process.
K-13	Knowledge of system monitoring and diagnostic tools and processes.	Explain the use of system monitoring and diagnostic tools.
K-14	Awareness of the components of the risk management process (e.g., methods for assessing and mitigating risk).	Interpret the importance of Controlled Access to mitigate risk and vulnerabilities in all network environments.
K-52	Knowledge of crisis management processes and procedures.	Explain crisis management processes and procedures.

K-33	Knowledge of the operations and processes for incident, problem, and event management including escalation as needed.	Enumerate the best technologies to support and solve actual technical support problems. Identify the common troubleshooting methods to solve a customer problem. Describe how to troubleshoot and repair a non-functioning device of a customer.
K-36	Knowledge of successful capabilities to identify the solutions to less common and more complex system problems.	
K-46	Knowledge of when to escalate to vendor or providers and how to monitor progress through solution.	
K-26	Knowledge of industry best practices for service desk (e.g., machine learning and AI).	
K-7	Knowledge of technical support operations, issues, and constraints.	
K-37	Knowledge of principles and processes for providing customer and personal services. This includes customer needs assessment, knowledge assessment, meeting quality standards for services, and evaluation of customer satisfaction.	
K-39	Knowledge of troubleshooting methods.	
K-40	Knowledge of change control procedures.	
K-51	Knowledge of case management tools, processes, and procedures.	
K-4	Knowledge of practices of internal, external, and global customers (as applicable).	
K-6	Knowledge of customer support processes and practices.	
K-3	Knowledge of operating environments, organizational software and ap	Describe different types of file extensions. Explain command line interface operating system commands. Discuss system administration concepts for various operating systems.
K-23	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).	
K-25	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	
K-16	Knowledge of cybersecurity and privacy principles.	Explain data privacy laws with respect to federal and state laws in the USA. Describe laws, regulations, and ethical behavior for cybersecurity
K-15	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	
K-18	Knowledge of specific operational impacts of cybersecurity lapses.	Discuss the consequences of cybersecurity lapses to an organization in light of organizational security policies, including automated functions.
K-27	Knowledge of organizational security policies.	
K-47	Knowledge of cybersecurity trends and effect of changes due to cybersecurity event.	
K-50	Knowledge of professional services automation and management (e.g., security patches that are automatically deployed).	
K-29	Knowledge of Personally Identifiable Information (PII) data security standards.	Discuss data security standards in depth as they pertain to different business and industry environments. Describe how to assess network vulnerabilities and attacks. Identify hardware and software defenses needed to protect the infrastructure in both wired and wireless installations.
K-30	Knowledge of Payment Card Industry (PCI) data security standards at an awareness level.	
K-31	Knowledge of Personal Health Information (PHI) data security standards.	
K-17	Knowledge of cyber threats and vulnerabilities.	
K-49	Knowledge of security threats.	
K-42	Knowledge of technical presentation tools.	Demonstrate effective oral, written, and presentation communication skills in the delivery of customer service, project planning and task completion in the technology support environment. Identify key organizational methods for continuous quality improvement and change management.
K-38	Knowledge of the structure and content of the English language including the meaning and spelling of words, rules of composition, and grammar.	
K-43	Knowledge of continuous quality improvement.	
K-48	Knowledge of change management approaches and communication.	

	Skills	Student Learning Outcomes
S-12	Skill in monitoring workload, managing time, and prioritizing requests.	Create a basic schedule for handling technical job requests based on deadlines and urgency. Configure network software and hardware equipment based on industry standards and specifications. Demonstrate practical skills in the selection and utilization of hardware and software tools to diagnose, repair, and optimize computer systems. Conduct research to troubleshoot client-level problems. Apply troubleshooting skills to solve a technical support problem. Use appropriate network performance monitoring tools to identify and solve system issues.
S-4	Skill in configuring and validating network workstations and peripherals in accordance with approved standards and/or specifications.	
S-2	Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system.	
S-3	Skill in conducting research for troubleshooting novel client-level problems.	
S-8	Skill in recognizing a problem and figuring out the best way to solve it.	
S-9	Skill in thinking about the pros and cons of different ways to solve a pr	
S-1	Skill in identifying possible causes of degradation of system performance or availability as well as skill in initiating actions needed to mitigate this degradation.	
S-13	Skill in adapting to and implementing change as a result of cybersecurity incident or AI directive.	Analyze the impact of cybersecurity incidents or directives and implement appropriate adaptive changes in security policies, procedures, or technologies. Demonstrate ability to effectively respond to on-premises or cloud-
S-5	Skill in incident response for on premises or cloud service models.	
S-6	Skill in communicating with others.	Demonstrate collaboration and communication skills to improve team productivity and customer support. Identify and interpret relevant technical information from multiple sources.
S-7	Skill in listening to others, not interrupting, and asking good questions.	
S-10	Skill in writing for communicating with co-workers or customers.	
S-11	Skill in reading work-related technical information.	
S-14	Skill in applying techniques for handling unhappy customers professionally.	Adapt communication and problem-solving approaches based on the specific nature of the complaint, demonstrating composure in challenging situations.
S-15	Skill in communicating with a customer at a level they can comprehend.	
	Abilities	**Student Learning Outcomes**
A-2	Ability to accurately define incidents, problems, and events in the trouble ticketing system.	Diagnose and document responses to maintenance and trouble tickets by following SOP. Evaluate issues not addressed by the SOP, and update necessary steps and knowledge databases as needed. Demonstrate consistent adherence to organizational SOPs, ensuring tasks are executed accurately and efficiently within established guidelines.
A-3	Ability to follow, develop, update, and/or maintain standard operating procedures (SOPs).	
A-9	Ability to record data in knowledge bases using proper keywords.	
A-14	Ability to use rules to solve problems.	
A-5	Ability to translate technical language into lay terminology when needed.	Communicate technical jargon in simple terms to clients. Explain complex problems and refer to appropriate higher technical support levels.
A-7	Ability to communicate complex technical issues and business implications.	
A-4	Ability to find solutions to less common and more complex system problems including escalating problems when needed.	
A-13	Ability to make order out of ambiguity.	Detect and identify the customer issue, considering all details and addressing ambiguities. Manage the details of the customer troubleshooting issue.
A-1	Ability to analyze and interpret customer input for expressed and implied issues.	
A-11	Ability to recognize and understand details.	
A-6	Ability to communicate verbally, appropriately for different audiences and organizational levels.	Demonstrate competence in effective collaboration, communication (both oral and written), and listening skills to define and solve technical problems for a diverse audience. Identify, evaluate, and suggest solutions to technical problems encountered.
A-10	Ability to listen and understand what people say.	
A-12	Ability to speak clearly.	
A-15	Ability to communicate by writing.	
A-16	Ability to create appropriate presentation visuals for technical material.	Communicate and present technical information. Analyze and interpret technical documents and diagrams. Analyze the impact of emerging technologies and adapt accordingly.
A-8	Ability to read and interpret technical documents, diagrams, and decision trees.	
A-17	Ability to adjust to changing technology.	

Technical Support Degree Expectations

A pool of 36 community college and four-year university faculty members from across the country were asked to categorize each knowledge, skill, ability, and task below. The question posed to them: would these KSA+Ts be reasonably included in a two-year AAS program, a four-year Bachelor's program, both, or neither? These results provide another tool for educators to use in assessing how to best incorporate each knowledge, skill, ability, and task.

		% Best Estimate			
	Tasks	2 Year AAS	Both 2 yr AAS and 4 yr Academic Degree	4 Year Academic Degree	Number of responses
T-1	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	37%	51%	11%	35
T-2	Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.	50%	44%	6%	36
T-3	Manage changes/updates for both internal and external customers when policies and procedures change.	25%	61%	14%	36
T-4	Maintain computer hardware.	56%	44%	0%	36
T-5	Provide technical support for software maintenance or use.	42%	53%	6%	36
T-6	Troubleshoot system hardware and software.	39%	58%	3%	36
T-7	Diagnose and resolve customer reported system incidents, problems, and events.	25%	67%	8%	36
T-8	Identify, test and implement solutions to computer hardware and software problems or escalate if required.	36%	58%	6%	36
T-9	Test software performance in relation to troubleshooting.	19%	61%	19%	36
T-10	Test computer hardware performance in relation to troubleshooting.	28%	64%	8%	36
T-11	Collaborate with others to resolve information technology issues.	17%	81%	3%	36
T-12	Identify and escalate issues to improve computer or information systems.	33%	61%	6%	36
T-13	Escalate computer hardware and software problems according to organization policies.	33%	56%	11%	36
T-14	Monitor and report client-level computer system performance.	33%	47%	19%	36
T-15	Monitor computer system performance to ensure proper operation.	28%	58%	14%	36
T-16	Assess or monitor system for cyberattacks.	11%	58%	31%	36
T-17	Responds to crises/security incidents following SOPs.	11%	58%	31%	36
T-18	Learn continuously about emerging industry or technology trends (e.g., machine learning and AI).	6%	67%	28%	36
T-19	Administer accounts, network rights, and access to systems and equipment.	25%	58%	17%	36
T-20	Perform asset management/inventory of information technology (IT) resources.	22%	61%	17%	36
T-21	Maintain incident tracking and solution database.	19%	61%	19%	36
T-22	Effectively document operational activities and enter results into the knowledge base and/or ticketing systems.	23%	66%	11%	36
	Knowledge				
K-1	Knowledge of the basic operation of computers.	31%	69%	0%	36
K-2	Knowledge of computer networking concepts and protocols, and network security methodologies.	28%	72%	0%	36
K-3	Knowledge of operating environments, organizational software and applications.	25%	67%	8%	36
K-4	Knowledge of practices of internal, external, and global customers (as applicable).	17%	56%	28%	36
K-5	Knowledge of internal organizational communication processes.	17%	77%	6%	35
K-6	Knowledge of customer support processes and practices.	31%	67%	3%	36
K-7	Knowledge of technical support operations, issues, and constraints.	25%	72%	3%	36

K-8	Knowledge of business issues regarding software licensing .	11%	56%	33%	36
K-9	Knowledge of interrelation between different organizational groups.	12%	49%	39%	33
K-10	Knowledge of organization chart and roles/responsibilities of company personnel/departments.	11%	63%	26%	35
K-11	Knowledge of preventative maintenance procedures and processes.	22%	72%	6%	36
K-12	Knowledge of applicable backup and restoration procedures.	17%	72%	11%	36
K-13	Knowledge of system monitoring and diagnostic tools and processes.	22%	72%	6%	36
K-14	Awareness of the components of the risk management process(e.g., methods for assessing and mitigating risk).	11%	43%	46%	36
K-15	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	3%	64%	33%	36
K-16	Knowledge of cybersecurity and privacy principles.	6%	83%	11%	36
K-17	Knowledge of cyber threats and vulnerabilities.	6%	86%	8%	36
K-18	Knowledge of specific operational impacts of cybersecurity lapses.	3%	69%	28%	36
K-19	Knowledge of measures or indicators of system performance and availability.	6%	66%	29%	35
K-20	Knowledge of systems administration concepts.	11%	71%	17%	36
K-21	Knowledge of physical computer components and architectures, including the functions of various components and peripherals.	33%	64%	3%	36
K-22	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).	33%	67%	0%	36
K-23	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).	28%	72%	0%	36
K-24	Knowledge of Cloud-based technologies and concepts (e.g. IAAS, SAAS, PAAS, file/sync/share).	8%	72%	19%	36
K-25	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	17%	81%	3%	36
K-26	Knowledge of industry best practices for service desk (e.g. Machine learning and AI).	17%	53%	31%	36
K-27	Knowledge of organizational security policies.	14%	86%	0%	36
K-28	Knowledge of remote access processes, tools, and capabilities related to customer support.	31%	61%	8%	36
K-29	Knowledge of Personally Identifiable Information (PII) data security standards.	12%	74%	15%	34
K-30	Knowledge of Payment Card Industry (PCI) data security standards at an awareness level.	12%	61%	27%	33
K-31	Knowledge of Personal Health Information (PHI) data security standards.	9%	64%	27%	33
K-32	Knowledge of an organization's information classification program and procedures for information compromise.	9%	56%	35%	34
K-33	Knowledge of the operations and processes for incident, problem, and event management including escalation as needed.	23%	66%	11%	36
K-34	Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.	25%	67%	8%	36
K-35	Knowledge of procedures used for documenting and querying reported incidents, problems, and events.	19%	67%	14%	36
K-36	Knowledge of successful capabilities to identify the solutions to less common and more complex system problems.	6%	40%	54%	35
K-37	Knowledge of principles and processes for providing customer and personal services. This includes customer needs assessment, knowledge assessment, meeting quality standards for services, and evaluation of customer satisfaction.	11%	54%	34%	36

K-38	Knowledge of the structure and content of the English language including the meaning and spelling of words, rules of composition, and grammar.	11%	86%	3%	36
K-39	Knowledge of troubleshooting methods.	19%	78%	3%	36
K-40	Knowledge of change control procedures.	11%	69%	19%	36
K-41	Knowledge of documentation processes and procedures.	8%	86%	6%	36
K-42	Knowledge of technical presentation tools.	11%	81%	8%	36
K-43	Knowledge of continuous quality improvement.	8%	61%	31%	36
K-44	Knowledge of VOIP telecommunication systems, both cloud based and on premise, as well as the OSI model and common networking protocols.	18%	77%	6%	34
K-45	Knowledge of what is cloud based and what is on premises as well as the different support models for each.	17%	67%	17%	36
K-46	Knowledge of when to escalate to vendor or providers and how to monitor progress through solution.	27%	53%	21%	34
K-47	Knowledge of cybersecurity trends & effect of changes due to Cybersecurity event.	6%	72%	22%	36
K-48	Knowledge of change management approaches and communication.	11%	56%	33%	36
K-49	Knowledge of security threats.	6%	92%	3%	36
K-50	Knowledge of professional services automation and management (e.g. security patches that are automatically deployed).	8%	67%	25%	36
K-51	Knowledge of case management tools, processes and procedures.	8%	58%	33%	36
K-52	Knowledge of crisis management processes and procedures.	8%	61%	31%	36
Skills					
S-1	Skill in identifying possible causes of degradation of system performance or availability as well as skill in initiating actions needed to mitigate this degradation.	20%	49%	31%	35
S-2	Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system.	42%	50%	8%	36
S-3	Skill in conducting research for troubleshooting novel client-level problems.	25%	61%	14%	36
S-4	Skill in configuring and validating network workstations and peripherals in accordance with approved standards and/or specifications.	25%	67%	8%	36
S-5	Skill in incident response for on premises or cloud service models.	18%	68%	15%	34
S-6	Skill in communicating with others.	6%	94%	0%	36
S-7	Skill in listening to others, not interrupting, and asking good questions.	6%	92%	3%	36
S-8	Skill in recognizing a problem and figuring out the best way to solve it.	6%	94%	0%	36
S-9	Skill in thinking about the pros and cons of different ways to solve a problem.	6%	91%	3%	36
S-10	Skill in writing for communicating with co-workers or customers.	9%	89%	3%	36
S-11	Skill in reading work-related technical information.	6%	92%	3%	36
S-12	Skill in monitoring workload, managing time, and prioritizing requests.	6%	83%	11%	36
S-13	Skill in adapting to and implementing change as a result of cybersecurity incident or AI directive.	6%	47%	47%	34
S-14	Skill in applying techniques for handling unhappy customers professionally.	3%	89%	9%	35
S-15	Skill in communicating with a customer at a level they can comprehend.	3%	94%	3%	36
Abilities					
A-1	Ability to analyze and interpret customer input for expressed and implied issues.	17%	80%	3%	35

A-2	Ability to accurately define incidents, problems, and events in the trouble ticketing system.	25%	72%	3%	36
A-3	Ability to follow, develop, update, and/or maintain standard operating procedures (SOPs).	6%	77%	17%	35
A-4	Ability to find solutions to less common and more complex system problems including escalating problems when needed.	11%	78%	11%	36
A-5	Ability to translate technical language into lay terminology when needed.	11%	86%	3%	35
A-6	Ability to communicate verbally, appropriately for different audiences and organizational levels.	11%	77%	11%	35
A-7	Ability to communicate complex technical issues and business implications.	9%	49%	43%	35
A-8	Ability to read and interpret technical documents, diagrams, and decision trees.	14%	71%	14%	35
A-9	Ability to record data in knowledge bases using proper key words.	11%	86%	3%	36
A-10	Ability to listen and understand what people say.	8%	92%	0%	36
A-11	Ability to recognize and understand details.	6%	92%	3%	36
A-12	Ability to speak clearly.	6%	92%	3%	36
A-13	Ability to make order out of ambiguity.	3%	85%	12%	34
A-14	Ability to use rules to solve problems.	8%	83%	8%	36
A-15	Ability to communicate by writing.	6%	92%	3%	36
A-16	Ability to create appropriate presentation visuals for technical material.	3%	86%	11%	36
A-17	Ability to adjust to changing technology.	6%	92%	3%	36