CoLAB TalentReady IT Pathways
Cyber Technologist KSAs for Curriculum Alignment

2. Cybersecurity Fundamentals

	KSA Description	Knowledge, Skill, or Ability?	Bloom's Taxonomy Level?	Cross-cutting KSAs	Notes
a	Examine and employ principles of Cybersecurity.	Ability	2	Cyber Security Specialist 2a	
a.1	Identify the goals, objectives and purposes of cybersecurity.	Knowledge	1		
a.2	Understand the basic principles of risk management.	Knowledge	2		
a.3	Describe the concepts of malware attack vectors.	Knowledge	1		
a.4	Maintain data security using data labeling, handling and, disposal as prescribed by policy and law.	Skill	3		
a.5	Mitigate threats by remaining abreast of industry information (CVE, CWE, threat intel feeds, ATT&CK Framework).	Skill	2	Cyber Security Specialist 2h	
a.6	Identify types of controls (e.g., Deterrent, Preventive, Detective, Compensating, Technical, and Administrative).	Knowledge	1		
b	Describe the need for security and explain security risks and security safeguards.	Knowledge	2		
b.1	Explain the need for confidentiality, integrity, and availability (CIA) of information.	Knowledge	1	Cyber Security Specialist 2b	
b.2	Describe authentication, authorization, and auditing(AAA).	Knowledge	2		
b.3	Explain data security in terms of authentication, authorization, access and auditing.	Knowledge	3	Cyber Security Specialist 2c, Networking 4g, Software Development 1l	
b.4	Understand the key cybersecurity principles in network defense (defense in depth, minimizing exposure, etc.).	Knowledge	2	Cyber Security Specialist 6f	
b.5	Identify security risks and describe associated safeguards and methodologies (e.g., auditing).	Knowledge	2		
b.6	Describe major threats to computer systems (e.g., insider threats, viruses, worms, spyware, ransomware, spoofing, hacking, social engineering, phishing).	Knowledge	2	Cyber Security Specialist 2d	
b.7	Describe the components of the physical environment (e.g., wiring closets, server rooms) and physical security systems.	Knowledge	2	Cyber Security Specialist 2e	
b.8	Describe the need for security in networking (e.g., firewall, access controls, encryption, demilitarized zone).	Knowledge	2	Cyber Security Specialist 2f	
b.9	Describe the need for security in application development.	Knowledge	2	Cyber Security Specalist 2g	
b.10	Track and catalogue physical assets **(**inventory, visibility**)**.	Ability	1		
b.11	Describe computer forensics, its importance in information security and cybersecurity, and its relevance to law enforcement.	Knowledge	2		
b.12	Identify the need for personal security in digital information and describe how personal information can be safeguarded.	Knowledge	2		
c	Understand the purpose and function of cybersecurity technology identifying the tools and systems that reduce the risk of data breaches while enabling vital organization practices. (Cybersecurity functions)	Knowledge	2		
d	Implement systems, apply tools, and use concepts to minimize the risk to an organization's cyberspace to address cybersecurity threats.	Ability	3		
e	Understand processes and tools of Vulnerability Assessment/Scanning.	Knowledge	2		
f	Categorize system controls according to industry standards (FISMA, PCI,**...)** .	Knoweldge	4		