Exam: Cyber Defense Specialist
Exam Link: https://knowledge-pillars.com/cyber-defence-specialist/

Course: Digital Forensics

TEKS Code & Standard	TEKS Description	Corresponding Cyber Defense Specialist Exam Objective(s)	Alignment Description
§127.793(c)(1)(E)	Explain ethical and legal responsibilities in relation to the field of digital forensics.	9 - Cyber Ethics, Law & Professional Practice	Understanding legal boundaries and ethical considerations in cybersecurity practices.
§127.793(c)(3)(A)	Recognize and analyze ethical and current legal standards, rights, and restrictions related to digital forensics.	9 - Cyber Ethics, Law & Professional Practice	Analyzing ethical and legal standards pertinent to cybersecurity operations.
§127.793(c)(4)(B)	Identify and describe types of cybercrimes and attack vectors.	1 - Cybersecurity Fundamentals & Threat Landscape	Understanding various cyber threats and their methodologies.
§127.793(c)(5)(A)	Use open-source tools to identify indicators of compromise.	8 - Incident Response & Digital Forensics	Applying tools like Autopsy and Volatility for forensic analysis.
§127.793(c)(6)(C)	Create, review, and edit a report summarizing technical findings.	8 - Incident Response & Digital Forensics	Documenting and reporting findings from digital investigations.

Course: Advanced Cloud Computing

TEKS Code & Standard	TEKS Description	Corresponding Cyber Defense Specialist Exam Objective(s)	Alignment Description
§127.689(c)(1)(A)	Describe the benefits and risks of cloud computing.	6 - Risk Management & Governance	Assessing cloud computing risks and implementing governance strategies.
§127.689(c)(2)(B)	Identify and describe major types of cloud computing services.	7 - Security Monitoring & Tooling	Understanding cloud services to implement appropriate security monitoring tools.
§127.689(c)(3)(C)	Implement cloud-based solutions using best practices.	2 - Networking Essentials for Security	Applying networking principles in cloud environments for secure configurations.
§127.689(c)(4)(D)	Analyze and troubleshoot cloud computing issues.	7 - Security Monitoring & Tooling	Monitoring and resolving security issues within cloud infrastructures.
§127.689(c)(5)(E)	Evaluate cloud computing solutions for business applications.	6 - Risk Management & Governance	Assessing the suitability and security of cloud solutions for organizational needs.

Course: Networking

TEKS Code & Standard	TEKS Description	Corresponding Cyber Defense Specialist Exam Objective(s)	Alignment Description
§130.305(c)(2)(A)	Configure and verify IPv4/IPv6 addressing and subnets.	2 - Networking Essentials for Security	Setting up network configurations essential for secure communications.
§130.305(c)(3)(B)	Interpret packet captures to spot anomalies.	2 - Networking Essentials for Security	Analyzing network traffic using tools like Wireshark to detect security issues.
§130.305(c)(4)(C)	Implement network security measures and protocols.	2 - Networking Essentials for Security	Applying security protocols to protect network integrity.
§130.305(c)(5)(D)	Troubleshoot and resolve network connectivity issues.	7 - Security Monitoring & Tooling	Identifying and addressing issues that may compromise network security.
§130.305(c)(6)(E)	Develop and implement a disaster recovery plan.	6 - Risk Management & Governance	Preparing strategies to recover from cybersecurity incidents.