LEVEL I CERTIFICATE & AAS, COMPUTER INFORMATION SYSTEMS AND SECURITY

Additional information: Reference the SHSU Polytechnic College (https://sam.edu/) page for additional information.

Program Description

The Computer Information Systems and Security AAS & Computer Support Specialist Level I Certificate is a workforce program designed to equip students with the knowledge and technical skills to work as computer support specialists with a focus on information security. The program coursework focused on computer support is designed to equip students with the skills and knowledge necessary to provide technical assistance to computer users in various settings. User support-focused courses in this program cover the fundamental concepts of computer hardware, software, networks, and customer service. Students will learn how to troubleshoot common computer problems, provide technical support, and ensure effective communication with end-users. The need for information security in the computer support field is growing rapidly. This program addresses the growing need of IT service providers to enhance security and mitigate cyber threats for end-users. The information security-focused coursework in this program will provide students with the skills necessary for protecting computer systems, networks, and data from cyber threats to ensure the integrity, confidentiality, and availability of information. Through hands-on labs, applied coursework, and industry-relevant projects, the program covers a wide range of topics in computer system support and cybersecurity, preparing students for the growing demand for information security professionals in various industries, including government, healthcare, finance, and technology. Graduates with the Level I Certificate credential will be able to enter the IT industry as a computer user support specialist. Graduates with the Associate of Applied Science credential will be able to evaluate and provide guidance for system and network security, design and install secure network systems, and monitor and maintain network traffic and security.

This Undergraduate Certificate is eligible to receive Title IV funding – Direct Loans, Pell Grant, SEOG Grant, and Federal Work Study. To be considered for aid, students need to submit a Free Application for Federal Student Aid (FAFSA).

Statewide Industry Insights

- Current Workforce: 31,931
- Average Salary: $91,700
- Open Positions: 2,895
  Data provided by Lightcast, 2024

Code	Title	Hours
Level I Certificate, Computer Support Specialist		
CPMT 1305	IT Essentials 1: PC Hardware and Software	3
ITNW 1309	Fundamentals of Cloud Computing	3
ITNW 1325	Fundamentals of Networking Technologies	3
ITSC 1305	Introduction to PC Operating Systems	3
ITSE 1359	Introduction to Scripting Languages	3
ITSY 1300	Fundamentals of Information Security	3
ITSY 1342	Information Technology Security	3
ITSY 2300	Operating System Security	3
ITSY 2301	Firewalls and Network Security	3
Total Hours		**27**

Note: The Level I certificate program stacks into the AAS curriculum.

Code	Title	Hours
AAS, Computer Information Systems and Security		
COMS 2382	Communication for Business & the Professions [1]	3
ENGL 1301	Composition I [2]	3
MATH 1332	College Mathematics [3]	3
MCOM 1330	Media, Culture and Society [4]	3
PHIL 2303	Critical Thinking [5]	3
CPMT 1305	IT Essentials 1: PC Hardware and Software	3
ITNW 1309	Fundamentals of Cloud Computing	3
ITNW 1325	Fundamentals of Networking Technologies	3
ITSC 1305	Introduction to PC Operating Systems	3

ITSC 1316	Linux Installation and Configuration	3
ITSC 1342	Shell Programming	3
ITSE 1359	Introduction to Scripting Languages	3
ITSY 1300	Fundamentals of Information Security	3
ITSY 1342	Information Technology Security	3
ITSY 2300	Operating System Security	3
ITSY 2301	Firewalls and Network Security	3
ITSY 2330	Intrusion Detection	3
ITSY 2341	Security Management Practices	3
ITSY 2342	Incident Response & Handling	3
ITSY 2345	Network Defense & Countermeasu	3
Total Hours		**60**

[1]   COMS 2382 satisfies the Core Curriculum requirement for Component Area IX (Component Area Option).
[2]   ENGL 1301 satisfies the Core Curriculum requirement for Component Area I (Communications).
[3]   MATH 1332 satisfies the Core Curriculum requirement for Component Area II (Mathematics).
[4]   MCOM 1330 satisfies the Core Curriculum requirement for Component Area IV (Language, Philosophy, and Culture).
[5]   PHIL 2303 satisfies the Core Curriculum requirement for Component Area VIII (Social and Behavioral Sciences).

Additional information: Reference the SHSU Polytechnic College (https://sam.edu/) page for additional information.

Level I Certificate, Computer Support Specialist

First Year

Fall	Hours	Spring	Hours
Term 1		Term 3	
CPMT 1305	3	ITSE 1359	3
ITSY 1300	3	ITSY 2300	3
ITSC 1305	3	ITSY 2301	3
Term 2			
ITNW 1309	3		
ITNW 1325	3		
ITSY 1342	3		
	18		**9**

Total Hours: 27

Note: The Level I certificate program stacks into the AAS curriculum. All courses are scheduled for 7.5-weeks in length.

AAS, Computer Information Systems and Security

First Year

Fall	Hours	Spring	Hours	Summer	Hours
Term 1		Term 3		Term 5	
CPMT 1305	3	ITSE 1359	3	MATH 1332 or 1314[1]	3
ITSY 1300	3	ITSY 2300	3	PHIL 2303[2]	3
ITSC 1305	3	ITSY 2301	3	Term 6	
Term 2		Term 4		ENGL 1301[3]	3
ITNW 1309	3	ITSC 1316	3	MCOM 1330[4]	3
ITNW 1325	3	ITSC 1342	3		
ITSY 1342	3	ITSY 2341	3		
	18		**18**		**12**

Second Year

Fall	Hours
Term 7	
COMS 2382[5]	3
ITSY 2330	3

ITSY 2342	3	
Term 8		
ITSY 2345	3	
	12	

Total Hours: 60

Note: All courses are scheduled for 7.5-weeks in length.

[1] MATH 1332 satisfies the Core Curriculum requirement for Component Area II (Mathematics).

[2] PHIL 2303 satisfies the Core Curriculum requirement for Component Area VIII (Social and Behavioral Sciences).

[3] ENGL 1301 satisfies the Core Curriculum requirement for Component Area I (Communications).

[4] MCOM 1330 satisfies the Core Curriculum requirement for Component Area IV (Language, Philosophy, and Culture).

[5] COMS 2382 satisfies the Core Curriculum requirement for Component Area IX (Component Area Option).

The Texas Higher Education Coordinating Board (THECB) marketable skills initiative is part of the state's **60x30TX plan** and was designed to help students articulate their skills to employers. Marketable skills are those skills valued by employers and/or graduate programs that can be applied in a variety of work or education settings and may include interpersonal, cognitive, and applied skill areas.

The Level I Certificate and AAS Program in Computer Information Systems and Security is designed to provide graduates with the following marketable skills:

- Firewall configuration and management, intrusion detection systems, intrusion prevention systems.
- Operating systems administration and management, Windows server security, Linux system administration and hardening, cloud infrastructure administration and security.
- Network discovery, security auditing, and basic scripting.
- Implementation of secure protocols, log analysis, security information, and event management.
- Security audits, risk assessment, and risk management protocols.

Computer Maintenance Technician

CPMT 1305. IT Essentials 1: PC Hardware and Software. 3 Hours.
Provides comprehensive overview of computer hardware and software and an introduction to advanced concepts addressed by Cisco certification. Topics may adapt to changes in industry practices.

Data Processing

ITSC 1305. Introduction to PC Operating Systems. 3 Hours.
Introduction to personal computer operating systems including installation, configuration, file management, memory and storage management, control of peripheral devices, and use of utilities.

ITSC 1316. Linux Installation and Configuration. 3 Hours.
Introduction to Linux operating system. Includes Linux installation, basic administration, utilities and commands, upgrading, networking, security, and application installation. Emphasizes hands-on setup, administration, and management of Linux.

ITSC 1342. Shell Programming. 3 Hours.
Reading, writing, and debugging shell scripts. Development of scripts to automate frequently executed sequences of commands. Covers conditional logic, user interaction, loops, and menus to enhance the productivity and effectiveness of the user. Intended for programmers who are familiar with operating environments and reading and writing various shell scripts.

Information Science

ITNW 1309. Fundamentals of Cloud Computing. 3 Hours.
Introduction to cloud computing from a business and technical perspective, including cloud concepts, services, architecture, system integration, connectivity, data center migration, administration, security, compliance and technical support. Coverage includes preparation for industry certifications. Topics may adapt to changes in industry practices.

ITNW 1325. Fundamentals of Networking Technologies. 3 Hours.
Instruction in networking technologies and their implementation. Topics include the OSI reference model, network protocols, transmission media, and networking hardware and software.

Information Security

ITSY 1300. Fundamentals of Information Security. 3 Hours.
An introduction to information security including vocabulary and terminology, ethics, the legal environment, and risk management. Identification of exposures and vulnerabilities and countermeasures are addressed. The importance of appropriate planning, policies and controls is also discussed.

ITSY 1342. Information Technology Security. 3 Hours.
Instruction in security for network computer hardware, software, virtualization, and data, including physical security; backup procedures; relevant tools; encryption; and protection from viruses. Topics may adapt to changes in industry practices.

ITSY 2300. Operating System Security. 3 Hours.
Safeguard operating systems by demonstrating support skills and designing and implementing security processes. Identify security threats and monitor security implementations. Use best practices to configure operating systems to industry security standards.

ITSY 2301. Firewalls and Network Security. 3 Hours.
Identify elements of secure network design that may include segmentation, Firewall implementation or a combination thereof to mitigate various types of security threats and attacks. Use Best Practices to design, implement, monitor and manage a network security plan. Examine security incident postmortem reporting and ongoing network security activities.

ITSY 2330. Intrusion Detection. 3 Hours.
Computer information systems security monitoring, intrusion detection, and crisis management. Includes alarm management, signature configuration, sensor configuration, and troubleshooting components. Emphasizes identifying, resolving, and documenting network crises and activating the response team.

ITSY 2341. Security Management Practices. 3 Hours.
In-depth coverage of security management practices, including asset evaluation and risk management; cyber law and ethics issues; policies and procedures; business recovery and business continuity planning; network security design; and developing and maintaining a security plan.

ITSY 2342. Incident Response & Handling. 3 Hours.
In-depth coverage of incident response and incident handling, including identifying sources of attacks and security breaches; analyzing security logs; recovering the system to normal; performing postmortem analysis; and implementing and modifying security measures.

ITSY 2345. Network Defense & Countermeasu. 3 Hours.
This is a practical application and comprehensive course that includes the planning, design, and construction of defenses for a complex network that will sustain an attack, document events, and mitigate the effects of the attack.

Programming

ITSE 1359. Introduction to Scripting Languages. 3 Hours.
Introduction to scripting languages including basic data types, control structures, regular expressions, input/output, and textual analysis. Topics may adapt to changes in industry practices.