

Student Name: _____

Computer & Information Technologies: **Security+ (3 Total Credit Hrs)**

Maysville Community & Technical College

Open Admissions

Certificate

Terry Pasley, Program Coordinator

Phone: (606)-759-7141 ext. 66153 Office: A-300 Maysville Campus Admin. Building Email: terry.pasley@kctcs.edu

Academic Plan Code: 1101013409 Academic Program Code: ENTC

Certificate Requirements (3 Credit Hours)		Credit Hours	Semester Taken
CIT 180	Security Fundamentals	3	
Total		3	

Notes:

- It is the responsibility of the student to notify their Advisor of changes they have made to their class schedule. Failure to do so could result in a delayed graduation date or ineligibility for graduation. (*Examples: Online registration, drop/add, or change of class sequence.*)
- CIT 105 AND a Level I Networking Course (CIT 160, or 161, or 162) must be completed before enrolling into CIT 180; OR Consent of Instructor.**
- Certificates may also be completed prior to or while earning an AAS degree. (Refer to MCTC's CIT Program Website).
- In order to graduate and obtain a Certificate, a student must earn a minimum grade of "C" in ALL courses required by the Certificate.
- Required minimum ACT or COMPASS placement scores are listed below:

	Math	Reading	Writing
COMPASS	42 (Pre-Algebra)	80	64

Security+ Certificate Information

The **Security+ Certificate** offers students the opportunity to earn a credential demonstrating the fundamentals of information security. This certificate consists of the core skills that students need to effectively build and maintain information security systems. In addition, this certificate will provide a way for professionals currently in the industry to update their computer networking skills and for new students to show progress in the CIT program. The Security+ Certificate prepares students for the CompTia Security+ exam which is recognized by the computer industry around the world.

Upon completion of this Certificate program, the graduate can:

- Explain basic security concepts.
- Identify and explain appropriate use of security tools to facilitate security.
- Evaluate current security issues related to computer and network systems.
- Evaluate and select appropriate incident response procedures, disaster recovery, and risk identification techniques to ensure business continuity.
- Differentiate various malware and systems security threats against computers and networks.
- Explain the vulnerabilities and mitigations associated with computers and network devices.
- Explain the proper use of common tools for carrying out vulnerability assessments.
- Identify and describe potential application and data vulnerabilities, including buffer overflow, DLL injection, and SQL injection.
- Explain how host firewalls, malware protection, and updates are important to application and data security.
- Describe the importance of user accounts and associated permissions.
- Compare and discuss logical and physical access control security methods.
- Explain authentication models and identify components of each model.
- Summarize and explain general cryptography concepts.
- Demonstrate public and private key pairs for digital signing and encryption/decryption.

Total Credit Hours: 3