Minor in Cybersecurity
Program Guide

This minor course of study in cybersecurity provides students with foundational knowledge and skills in understanding, analyzing, and addressing various aspects of digital security. Through a combination of theoretical concepts and practical applications, students delve into topics such as network security, cryptography, ethical hacking, and risk management. They learn to identify vulnerabilities in systems, develop strategies to protect against cyber threats, and implement security measures to safeguard data and information assets. This minor equips students in **any area** major, with valuable expertise in an increasingly critical field, preparing them for careers in cybersecurity or complementing their primary areas of study with essential skills in digital defense. The minor is especially complimentary with programs dealing with technology or law enforcement or management.

The minor consists of 21 credits apportioned as follows:

- 18 required credits
- 3 elective credits

REQUIRED COURSES (18 s.h.)

Course #	Course Name	Credits	Course Notes/Attributes
CS 01211 or MIS 02315	Principles of Information Security	3	
CST 03201 or CS 03351	Security+ or Cyber Security: Fundamentals, Principles, and Applications	3	
CST 03215 or CST 03218	Penetration Testing Fundamentals or Ethical Hacking Fundamentals	3	
CST 09210 or CS 09410	Introduction to Computer Networks and Data Communications or Data Communications and Networking	3	
CS 03355 or MIS 02318	Cybersecurity, Management, Policy, and Risk or Information Systems Risk Management	3	
CST 03410	Cyber Defense	3	

ELECTIVE COURSES (must take one course from the following list - 3 s.h.)

Course #	Course Name	Credits	Course Notes/Attributes
CST 03252	Foundations of Computer Forensics	3	
CST 03270	Introduction to Intrusion Detection	3	
CST 06220	Linux/Unix Essentials	3	