

CYBERSECURITY MINOR

Arts and Technologies

Offered by the Cybersecurity Council

Council: A M A Elman Bashar, Christopher T. Drever, Laura Dykstra, Francis W. Williams, Zhizhang Shen

The Cybersecurity minor addresses the growing need of professionals in the field of cybersecurity. Cybercrime has become a significant global threat and concern of cybersecurity has evolved from a strictly technological challenge to a socio-economic issue. To address the multifaceted aspects of cybercrime and cybersecurity, this minor program aims to equip the students with necessary technical and legal backgrounds. The technology part of the program provides foundation for understanding key issues of protecting digital information, identifying threats and determining protection levels, response to security incidents, examination of pre- and post-incident procedures, and designing consistent, reasonable cyber security system, with appropriate intrusion detection and reporting features. The legal component covers the issues related to identification of common types of fraudulent schemes and the laws that have been enacted and developed specifically for combating cybercrime. Other topics may include, causes, victimization, legal issues, control strategies, and societal costs regarding the "cybercrime" problem.

Course	Title	Credits
Minor Requirements		
CJ 3015	Cybercrime	4
CJ 3405	Homeland Security	4
CS 2010	Computing Fundamentals (TECO)	3
CS 3420	Introduction to Cybersecurity	3
Electives		
Select one of the following:		3-4
BU 3240	Information Technology	
CJ 2405	White Collar Crime	
CJ 3005	Criminal Investigation	
CS 2370	Introduction to Programming	
CS 4420	Computer Security	
CS 4520	CyberEthics (DICO,INCO,WRCO)	
SO 2405	White Collar Crime	
Total Credits		17-18

The prerequisites for the courses in this minor can be found in the course descriptions in this Catalog.