The University of Akron
Disaster Science & Emergency Services

Course Title: Cyber Issues in Emergency Management and Homeland Security
Course Number: 2235: 435
Course Credit: 3 credit hours

Course Description:
Discussion and analysis of cyber issues impacting the public, private, and nonprofit sectors of emergency management and homeland security.

Program Outcomes:
Upon completion of this course, the student will gain a better understanding of:

1. the principles associated with cybersecurity
2. various threats associated with computers
3. utilization of case studies analyzing cyber issues in the public, private, and nonprofit sectors
4. emergency management fundamentals (preparedness, response, recovery, and mitigation) in regard to cyber issues

Course Rationale:
This nontechnical class will introduce the basic components of cyber issues and security as it relates to the public, private, and nonprofit sectors of emergency management and homeland security. This include
addition, the course will discuss concepts such as hacking, infrastructure vulnerability, and national security. The course is designed to promote critical thinking through applications which is a basis for learning rather than memorizing material.

Grading Scale

Grade	Percent Required
A	93-100%
A-	90-92%
B+	87-89%
B	83-86%
B-	80-82%
C+	77-79%
C	73-76%
C-	70-72%
D+	67-69%
D	63-66%
D-	60-62%
F	0- 59%

Program Assessment:
The University of Akron and specifically the Emergency Management program assesses student learning at several levels: general education, program, and classroom. The goal of these assessment activities is to improve student learning. As a student in this course, you will participate in various assessment activities. Students have an active role in course and program assessment projects designed to strengthen and constantly improve student learning and educational outcomes.

An example of your work, a paper, some test questions, a presentation, or other work may be selected for assessment. The data is run across classes and over years to generate information on how to make our program better.

Accessibility Statement:
If you feel you may need an accommodation or special service for
this class, please see the office of accessibility for assistance.

Course Outline:

Topic I: Principles of Cyber Security

Topic II: Public Sector

Topic III: Private Sector

Topic IV: Nonprofit Sector

Topic V: Vulnerabilities

Bibliography:

Amoroso, Edward. (2007). *Cyber Security*. Summit, NJ, Silicon Press, pp. 200.
ISBN: 0-929306-38-4

Andreasson, Kim J. (2011). *Cybersecurity: Public Threats and Responses*. Boca Raton, FL, CRC Press, pp. 392.
ISBN: 978-1-439-84663-6

Kostopoulos, George K. (2013). *Cyberspace and Cybersecurity*. Boca Raton, FL, CRC Press, pp. 236.
ISBN: 978-1-466-50133-1

Taylor, Robert W., Fritsch, Eric J., and Liederbach, John. (2014). *Digital Crime and Digital Terrorism (Third Edition)*. New York, Prentice Hall, pp. 408.
ISBN: 978-0-133-45890-9