Syllabus for CYB 705 Sociological Aspects of Cybersecurity

NOTE: This syllabus document contains the basic information of this course. The most current syllabus is available in the full course.

Course Description

Presents the principles of applied sociology that account for the human factors in security systems. Topics include an examination of the human role in cybersecurity, the role of security in the context of an organization, and a special focus on the development and implementation of cybersecurity policies.

Prerequisite(s)

None

Program Outcomes

This course addresses the following competencies and program outcomes of the Masters of Science in Cybersecurity:

- Program Outcome 9: Evaluate and create security policies and processes for an organization and apply appropriate security frameworks
- Program Outcome 10: Implement identity and access management controls
- Program Outcome 11: Assess trends in computer criminology and social behaviors related to technology use including physical security
- Program Outcome 12: Engage in ethical decision-making and apply ethical principles to cybersecurity

Course Outcomes

Upon completing this course, you will be able to do the following:

- Develop cybersecurity policies that are effective and ethical.
- Analyze security systems and solutions for weaknesses related to human interaction.
- Develop and implement effective security awareness training programs.
- Recognize the role of information assurance and security in the context of a larger organization.
- Explain the impact and influence of technology on human behavior, with emphasis on privacy and compliance.
- Develop appropriate identity and access management policies and recognize access control models.

Course Requirements/Components

Individual Assignments

There are four individual writing assignments in this course. The assignments either require you to conduct an analysis of a journal article provided by the instructor or to delve deeply into a particular topic. The assignments require you to conduct research on the topics being explored.

Group Assignments

There are two major group projects in this course. One project requires your group to develop a training program proposal, and the other requires you to develop a policy, procedure, standards, and guidelines document. These projects will require significant effort and coordination between your group members.

Mid-Term and Final Exams

There is a mid-term and final exam that contains questions closely aligned with the ethics questions found on the Certified Information Systems Security Professional (CISSP) exam.

Discussions

There are discussions related to the topic being explored that week. You are not required to participate in every discussion, but there is a participation grade for your involvement throughout the semester.

Course Outline

Module 01: Introduction to Social Theory

Module 02: The Role of Technology

Module 03: The Role of Information Assurance and Security

Module 04: Social Engineering – Hacking Humans

Module 05: Digital Citizenship in the Information Age

Module 06: Data Quality, Data Value, and the CIA Triad

Module 07: Civil Transgressions in a Digital Medium

Module 08: How Big Data Shapes Everyday Life

Module 09: Privacy as a Right in the Big Data Era

Module 10: The Role of Compliance

Module 11: The Future of Cybersecurity

Grading

The following grading scale will be used to evaluate all course requirements and to determine your final grade:

Grade	Percentage Range
A	90% or greater
A-	87% - < 90%

B+	83% - < 87%
B	80% - < 83%
B-	77% - < 80%
C+	73% - < 77%
C	70% - < 73%
C-	65% - < 70%
D	60% - < 65%
F	0 - < 60%

Assignments	Percentage
2 exams (mid-term and final) – 20% each	40%
2 Group Projects – 15% each	30%
4 Individual Assignments – 5% each	20%
Discussion Participation	10%
Total	100%