ITMS 534 SYLLABUS

ITMS 534 Human Factors in Cybersecurity

Hours: 3 credit hours / 60 contact hours

Instructor: Calvin Nobles, Ph.D.

Textbook, title, author, and year: *Human Factors in Simple and Complex Systems 3rd Edition,* Proctor, Robert W. and Trisha Van Zandt December 26, 2017, CRC Press; ISBN 9781482229561

Specific course information

a. **Catalog description:** This course introduces the applied theories relevant to human factors in information security, digitalization, and sociotechnical environments. Examines the human element through a comprehensive approach that explores human errors, new technologies, and cybersecurity incidents. Investigates human-related aspects that have an impact on the practices, policies, and procedures that are in place in an organization to secure the firm's information. Topic areas include human behavior, ethics, psychology, social engineering, the culture of hacking, cybercrimes, security fatigue, and burnout. The analysis covers techniques to prevent intrusions and attacks that threaten organizational data and methods to identify potential insider threats.
b. **Prerequisites: None.**

Specific goals for the course

a. **Course Outcomes:** Upon successful completion of this course, students should be able to recall and employ principles of human factors, human computer interaction, user interface design, and user experience to enhance cybersecurity in an enterprise setting though system error reduction, countering of social engineering techniques, and employment of human factors as an element of active cyber defense.
b. **Course student outcomes:**
Students completing this course will be able to:
   - Identify and articulate key human factors concepts
   - Identify human factors shortfalls in major data breaches and cybersecurity incidents.
   - Effectively evaluate human errors and mistakes using the Human Factors and Analysis Classification System to prevent/reduce such mistakes from occurring in the future.
   - Apply human factors principles to reduce high friction point in system designs and cybersecurity operations.
   - Describe and apply core theories, models and methodologies from the field of human factors.
   - Describe and discuss current research in the field of human factors.

Topics to be covered

a. User interface (UI) design (web, mobile, tablet)
b. Interaction Design & User Experience
c. Usability testing
d. Wireframing & Prototyping (Rapid, Paper, Interactive)
e. Storyboarding, Ideation
f. User-centered Design (UCD)
g. Cybersecurity Use Cases