Summer 2017 CSC Special Topics and Revised Course Descriptions

1. **CSC 8600 - 030 Object Oriented Design & Prog (revised description)**
   What is it about the object-oriented (OO) paradigm that's been so compelling for decades? Why did James Gosling, the creator of Java, indicate that he'd remove implementation inheritance ("extends") from the language given the chance to do it over? Does an OO design truly model the "real-world"? How can OO principles be applied to today's ecosystem of multi-paradigm languages?

   Explore these questions and more in this refreshed instance of the classic OO design and development course. Gain a deep understanding of core OO concepts, design principles and design patterns, plus hands-on experience with applying them to interesting problems that highlight the trade-offs inherent in all design activities. Through expert guidance and practical tips, students will learn how to design and develop adaptable and maintainable OO applications.

2. **CSC 9010 - 030 TOP:Machine Learning & Data Science**
   This course will cover topics in machine learning including these main three areas:
   a. Classification. Example – choose if a person is likely to develop cancer based on 30 attributes
   b. Clustering. Create classifications based on attributes. Example – identify subgroups of shoppers with similar attributes and the items they may buy.
   c. Numerical Prediction. Example – predict market value of a house based on a large set of attributes (zip code, square feet, etc.)

   The course will focus on understanding/use of algorithms, techniques, and tools. Assessment will include projects/reports/presentations. Programming environments include Python, R, and Weka.
   Background: Ability to understand mathematical notations. Specifically, from linear algebra and calculus. Proficiency with at least one high-level programming language.

3. **CSC 9010 - 031 TOP:Cyber Security**
   Cybersecurity can no longer be considered as only a technology problem relegated to the IT department. Disruption of services, theft of confidential and private information, malicious modifications impacting everything from manufacturing lines to election results are widespread and growing. The enemies are anonymous, asymmetric and reside globally, including in our own neighborhoods. Potential impacts to human safety, personal privacy, national security and the bottom line are very real. Domestic and foreign government agencies have made cyber-defense and cyber-warfare a top priority. Commercial and non-profit entities have also elevated the importance of cyber risk management. In recent years the largest investments at many of the top listed companies have been in cybersecurity. This is further underscored by the attention on cyber risk metrics at both the C-Suite and the board levels. With this new focus comes new expectations; workers at every level and across every function, are expected to be cybersecurity literate.
   The cybersecurity fundamentals course is designed to provide the student with a high-level overview of the issues, challenges and disciplines involved in the cyber-defense of information, physical assets, people, corporations and nations. A section of the course will include an overview of the risks, benefits and limitations of various technologies as they are both a source of risk and a means to detect and prevent attacks. A laymen understanding of computers, operating systems, databases, websites, networks, the Internet, cloud services and mobile devices is expected. However, specific in-depth technical knowledge, programming or hands-on technical experience is not a prerequisite.

This course is taught seminar style and is comprised of reading assignments, lectures, weekly research into data breaches and current events with summaries, in-class discussions and team exercises. Each student will have the opportunity to deep-dive into a specific topic or technical lab of interest and make a presentation to the class.
Sub-topics may include:

- The attackers: their motives, methods and means (Hacks and Attacks)
- The victims: the impacts, costs of a breach, the likelihood of a breach (Caused and Consequences)
- Data Privacy
- Cyber security threats and risks: what are they and how to assess them
- Cyber risk mitigation strategies – How to protect yourself
- Overview of technology vulnerabilities and vulnerability detection strategies
- Overview of policies, practices and technologies used in cyber risk mitigation
- Industry and national security issues and concerns
- How entities organize to address cybersecurity risk
- Future threats and the evolving cybersecurity landscape

4. **CSC 9010 - 032 TOP:Software Def Networks**
Introduces software-defined networking, addressing both underlying motivations and current implementations. Students will learn how software-defined networking techniques are becoming essential to modern data centers and cloud-based applications. Primary topics include:

- Traditional networking overview (OSI model, switching, routing, transport guarantees)
- Rationale for software-defined networking
- OpenFlow protocol
- Virtual switches and routers
- SDN controllers
- Containerization
- Container orchestration

Class sessions will be a mix of lecture material and hands-on exercises including contemporary SDN and cloud tools.

5. **CSC 9010 - 033 TOP:Containers & Micro Services**
Containers and Microservices technologies are the next advancement in highly scalable, performance-driven systems implementation. In this course, we will seek to understand Containers, what they are, and how they are used. Additionally, we will explore Microservices as an example of the kinds of services that may be hosted within Container technologies.

The course seeks to give the student a broad and high level of understanding & consideration when implementing decoupled, highly scalable, and highly available services. No previous understanding of Containers is required. However, strong software development knowledge is needed, since the focus of the course will assume that students are already knowledgeable in software development practices.

Finally, we will look at implementing and consuming such services from containers, examine the readiness perspective of the Enterprise, how these changes affect individual developers, organizations, and future software design & evolution. These ideas are the basis for Cloud Application Development practices.

Topics include:
• Containers
    - o High level overview of Container Technology

- Concepts in Technologies
- Impact of Container Technology in business and for developers
- Container Orchestration
- Working with Docker
- Implementing Docker Solutions

• Microservices
- What are Services?
- Emergence of Microservices
- Microservices Design
- Microservices Technologies

• Implementing Microservices & Containers
- Installing Microservices on Containers
- Implementing Docker Swarm
- Automation: A DevOps Approach

6. **CSC 9010 - 035 TOP:Health IT Security & Privacy (100% Distance Learning)**
Security and Privacy laws/ regulations, technology and practice. Course explores the complex sets of laws, rules and regulations in the United States that drive technology innovation and practices in the field of eHealth. The US laws and agencies include HIPPA, HITECH, FDA, FCC and agency departments such as the HHS Office of National Coordinator and Office of Civil Rights.

Topics include:

-Technology and practice in the areas of patient rights
-Electronic transmission of health data
-Unauthorized access, vulnerabilities, unsecured access
-Inadequate encryption, authentication failures, and other access control vulnerabilities
-Security risk assessment, privacy and security gaps in health information exchanges