

ISCI - INFORMATION SCIENCES (ISCI)

ISCI 1110 Cybersecurity Bootcamp (1 Credit)

This course provides students with the foundational knowledge required to begin studying cybersecurity and prepare for a career in this field. The students develop the knowledge of Enterprise Security principles that are common in today's business environment. This knowledge will be critical to success in the positions of Security Analyst, Network Security Engineer, and Risk Analyst. The material covers the fundamentals of cybersecurity, including risk management, network security, endpoint protection, disaster recovery, and business continuity. Prerequisites: The students must have basic Windows user skills, fundamental understanding of computer and networking concepts, and the ability to use Blackboard.

ISCI 1117 Computing for Informatics (3 Credits)

The course teaches the foundations of computing and programming in a scripting language, such as Python, Perl and Scala, for professions dealing with data and information, including cybersecurity, data science, and data and information engineering, and addresses the impact of information systems and cybersecurity on society. It teaches the fundamentals of programming for informatics, to solve problems in cybersecurity, data science applications, and information systems. The course focuses on the design process that leads students from a problem statement to a well-organized solution.

ISCI 1120 Network+ Prep (2 Credits)

This course focuses on the Network+ test principles and the material necessary to pass the CompTIA Network+ (N10 – 007) examination in Cybersecurity. The course conveys knowledge and understanding of networking concepts and acquire the required skills to prepare for a career in network support or administration, or who wish to prepare for the CompTIA Network+ certification exam.

ISCI 2130 Security+ Prep (3 Credits)

This course focuses on the Security+ test principles and the material necessary to pass the CompTIA Security+ examination in Cybersecurity. The students develop the knowledge of the Enterprise Security principles that are common in today's business environment. This knowledge will be critical to success in the positions of Network Security specialists. The course material discusses the common practices of security, network protection and the protection practices of industry.

ISCI 3111 Cybersecurity Law and Policy (3 Credits)

This course is a survey of legal and public policy issues arising from the problem of cybersecurity. It begins with a review of Internet law concepts, highlighting the importance of social norms and "soft law" in the Internet's development, while also recognizing the ways in which the Internet's minimal legal governance frameworks contribute to its security risks. It then focuses on computer crime law, including the U.S. Computer Fraud and Abuse Act, which contains provisions that address data theft and hacking. This discussion of computer crime leads to consideration of online privacy, government surveillance, and legal process for government investigations, and cyberwar. The final portion of the course covers legal and policy issues relating to private information infrastructure.

ISCI 4021 Cybersecurity Capstone (3 Credits)

Students participate in a collaborative cyber-security group project under the guidance of a faculty member in the cyber-security program. The topic of the project, chosen in consultation with the faculty member, is closely integrated with the learning experience in any of the courses offered in the cyber-security program. The project will focus on providing a solution to a real-world cyber-security issue that an actual or hypothetical organization may face.