SECURITY MANAGEMENT (SECM)

SECM 6001 Physical Protection Systems (3)
An introductory course to the systematic discipline of Physical Protection System design, implementation, and testing. The methodology presented is scalable for small, medium, and large security applications ranging from home security systems to safeguarding and securing sensitive nuclear facilities.

SECM 6002 Intro to Emergency Management (3)
This course will be an advanced examination of modern emergency management concepts, trends nationally and internationally, practical and political issues and policies, technological applications to emergency management, and the development and practical implementation of sound emergency management practices designed to protect people, communities, critical infrastructure and key assets. Included will be a brief review of emergency management policy and procedures in the United States and other countries, legal issues, social science perspectives, planning concepts and techniques, disaster modeling, operational problems, analytical methods, special populations, and management styles. Additionally, case studies will be examined to determine the extent of effective or ineffective planning, responding, and recovering from natural and technological disasters.

SECM 6003 Risk Mgt & Threat Assessment (3)
This course examines the concepts, methods, and practices associated with risk management and threat assessment from an all-hazard perspective. Students will learn how to conduct hazard and risk analysis for both the public and private sectors. This course will include identifying and profiling hazards, analyzing and assessing hazard risk developing tactics to manage risk, examining multiple risk assessment tools, and communicating risk to the public. Participants will examine critical infrastructure sectors and associated interdependencies, cascading consequences, and shared vulnerabilities. Students will perform their own risk analysis and develop recommendations for policy makers as part of this curriculum.

SECM 6004 Business Continuity (3)
With global business stretched across extended supply chains, productivity has increased, but it has come at a cost of increased vulnerability. Businesses cannot afford to be unprepared for traditional and emerging threats. Business continuity is a fast-growing area of emergency and security management focused on the private sector. This specialty works to ensure continuous business operations before, during, and after disasters or other normal disruptions. It is designed to provide strategies tied to national and international standards for the development of detailed business continuity plans. Students will discuss managing disruptions, maintaining continuity of critical operations, and mitigating losses that occur when interrupted. Based on the all-hazard framework, students will learn about the current threats, including political instability and cyber attacks. Regardless of the impetus for such disruptive events, students will be prepared to train employees to both mitigate and recover from such events. Students will also discuss best practices in the ongoing recovery efforts after an event.

SECM 6005 Corporate Security (3)
The intent of this course is to give students an overview of the varied objectives and duties associated with Corporate Security. The goal is to present the multiple levels, tasks and duties associated with Corporate Security as it applies to a U.S. based corporation, relative to employee safety and security as well as what is known as Executive Protection, and offering insight into the different career opportunities associated with this line of work.

SECM 6006 Financial Institution Security (3)
This course introduces the theory of providing security for financial institutions. Financial institution security refers to the various security measures for the purpose of protecting life and property, protecting the confidentiality of critical data and information and other financial assets. The course also reviews laws and regulations that guide security practices such as those promulgated by the Federal Trade Commission (FTC) and its Safeguards Rule amongst many other designs. This class will analyze the basics of this industry and review practical approaches to protecting them against threats such as theft, both internal and external, vandalism, data center security, cyber-crimes and fraud. Topics include the value of conducting security audits, conducting a business impact analysis, implementing security systems and interfacing with the public.

SECM 6007 Cyber Threats and Homeland Sec (3)
“Cyberspace” has become a pervasive presence in modern society, and a healthy functioning cyberspace is elemental to our economy and to national security. Along with benefits, however, there exists threats and malicious actors who seek to exploit cyberspace vulnerabilities, and, in doing so, threaten critical infrastructure and threaten National Security. This course will study the nature of cyber threats, including computer and digital crimes, information warfare and cyber terrorism, and related threats to personal, organizational, economic and national security. Students will gain an understanding of the variety and nature of cyber threats including digital espionage, computer break-ins, computer hacking, malware, communications eavesdropping, forgery, disruption to information flow, electronic bombs, cyber war and the growing presence of terrorist organizations on the internet. This course will also review countermeasures and a protection methodology to cyber threats, cyber security investigations, evidence gathering, and legal challenges. Lastly, this course will review current and national policies for securing cyberspace and the impact of cyber security on privacy and civil liberties.

SECM 6008 Sport/Event Security and Respo (3)
This course provides an overview of security planning, risk assessment methodologies, and emergency response considerations for sport and special events. Students will learn how to identify threats and vulnerabilities, analyze and mitigate risk, and harden events and venues through security countermeasure proposals and emergency response/recovery initiatives.
SECM 6009 Leadership in Security Mgt (3)
Security management practitioners must use leadership and influence effectively to lead organizations in planning for, preventing, and responding to crises and emergencies. This type of leadership encompasses vision, direction, coordination, and motivation. Leadership skills are necessary whether dealing with senior corporate officials, government partners, or the public. The lack of leadership during an emergency can result in the loss of life, property, and the public trust. This course will expose students to the major factors, theories, and strategies for leadership, influence, and decision-making. The traits, skills, and behaviors of effective leaders will also be discussed.

SECM 7001 Intelligence Anlysis and Critica (3)
This course is designed to give students an advanced understanding of intelligence-gathering and analysis as it relates to critical thinking; linkages to money laundering, risk management, risk assessment factors, operational concepts and strategic implications. It is a logical follow-on study that further examines the collaborative process of intelligence analysis and will provide homeland security professionals tools, framework and concepts to further develop their leadership skills by understanding how the synthesis and utilization of intelligence impacts decision making in tactical, operational and strategic settings while emphasizing the principles of holistic, all-hazards approach to preparedness.

SECM 7002 Approaches- Counter Terrorism (3)
Students will employ critical analysis to examine key policy issues and balances that must be addressed in strategic counterterrorism planning, particularly in the use of applied technology within the context of civil jurisdiction and rule of law. The course will examine terrorist threats to the homeland and how these threats can be met by the application of science and technology. Policy issues that address the balance between security and civil liberties that must be resolved to effectively counter terrorism will be discussed. These issues will be addressed from the governance perspective of a liberal democracy. Strategic planning principles that integrate capabilities of current and future applied technology and the key legal and policy issues that must be resolved in order to make effective use of information as balanced against civil liberties will be explored as well.

SECM 7003 Disaster Communications (3)
This course discusses historical and emerging issues that accompany communication and messaging during disaster and emergency situations. Students will analyze best practices, tools, and tactics for crisis and risk communication. Participants will have the opportunity to develop strategies and communication solutions for all audiences, including internal and external partners, the public, and social media.

SECM 7900 Capstone (3)
This course synthesizes the full range of knowledge, skills, and abilities students developed over the entirety of their security management studies. Students will integrate and apply key concepts through a business-based project, developing a proposal and conducting this project at a business or local government sector entity. At the end of the semester, the project will be presented to both the chosen organization and classmates. Students will integrate critical decision-making skills with a unique and local hands-on learning experience. A written report documenting all aspects of the project will be presented for faculty approval.