No Cost Cybersecurity Online Courses available at Texas A&M Engineering Extension Services (TEEX)

Cyber 101 - Two credit hours through ACE are provided only if all three courses within the Cyber 101 track are completed.		
Course No.	**Course Title**	**Description**
AWR168	Cyber Law and White-Collar Crime	This intermediate course is designed to teach students the fundamentals of computer crime issues from a legal perspective. The training will highlight the various computer crimes and appropriate response by first defenders and others that may encounter these types of issues. Participants learn legislations and organizational efforts to control or prevent such crimes. This course covers intellectual property law (copyright, trade secrets, unfair competition, and unfair business practices), personal jurisdiction, electronic commerce and software contracts, telecommunications, antitrust, privacy, the right to accuracy of information, the right to access information, and the First Amendment.
AWR174	Cyber Ethics	Cyber Ethics is designed to teach students the proper techniques with which to approach the difficult ethical dilemmas that arise from using the modern Internet. In addition to providing students with the skills to assess future ethical dilemmas for themselves, Cyber Ethics also looks at some of the more pressing concerns related to Internet usage today.
AWR175	Information Security for Everyone	Information Security for Everyone is designed to teach the principles and practices that all computer users need to keep themselves safe, both at work and at home. By presenting best practices along with a small amount of theory, trainees are taught both what to do and why to do it. Topics covered include how to secure both clean and corrupted systems, protecting your personal data, securing simple computer networks, and safe Internet usage.

Cyber 201 - Two credit hours through ACE are provided only if all four courses within the Cyber 201 track are completed.		
Course No.	**Course Title**	**Description**
AWR138	Network Assurance	Network Assurance covers secure network practices necessary to protect networked systems against attacks and exploits. Network security administration topics include firewalls, intrusion detection/prevention, common cryptographic ciphers, AAA (authentication, authorization, and accounting), server and client security, and secure policy generation.
AWR139	Digital Forensics Basics	This course covers investigative methods and standards for the acquisition, extraction, preservation, analysis, and deposition of digital evidence from storage devices. This course offers a wide array of forensics situations that are applicable to the real world. Students will learn how to find traces of illegal or illicit activities left on disk with computer forensics tools and manual techniques, and how to recover data intentionally hidden or encrypted by perpetrators.
AWR173	Information Security Basics	Information Security Basics is designed to teach entry and mid-level IT staff the technological fundamentals of information security. The goal of this course is to provide trainees some preliminary knowledge of computer security to help in identifying and stopping various cyber threats. In addition to providing an introduction to information assurance, trainees will also learn general concepts (terminologies), an overview of TCP/IP, introductory network security, introductory operating system security, and basic cryptography.
AWR178	Secure Software	This course covers secure programming practices necessary to secure applications against attacks and exploits. Topics covered include fundamental concepts of secure software development, defensive programming techniques, secure design and testing, and secure development methodologies.

<table>
<tr><td colspan="3">Cyber 301 - Two credit hours through ACE are provided only if all three courses within the Cyber 301 track are completed.</td></tr>
<tr><th>Course No.</th><th>Course Title</th><th>Description</th></tr>
<tr><td>AWR169</td><td>Cyber Incident Analysis and Response</td><td>This course covers various incident analysis tools and techniques that support dynamic vulnerability analysis and elimination, intrusion detection, attack protection, and network/resources repair. The trainee will be presented with real-world examples and scenarios to help provide knowledge, understanding, and capacity for effective cyber incident analysis and response.</td></tr>
<tr><td>AWR176</td><td>Disaster Recovery for Information Systems</td><td>Disaster Recovery for Information Systems will train business managers to respond to varying threats that might impact their organization's access to information. This course provides requisite background theory and recommended best practices needed by managers to keep their offices running during incidents of different types. Topics include an overview of business continuity planning; disaster recovery planning; guides for implementing and managing disaster recovery plans, a discussion of technical vulnerabilities faced by organizations, and an examination of legal issues that may confront an organization.</td></tr>
<tr><td>AWR177</td><td>Information Risk Management</td><td>This is an intermediate level course covering topics on information assets, identifying risks, and management processes highlighting best principles and practices. It will provide training on information risk-related tools and technologies (such as asset evaluation, business impact analysis, risk identification, risk quantification, risk response, security policies, and compliance) for better understanding of potential threats and vulnerabilities in business online, and learning to adopt levels of security measures and best practices.</td></tr>
</table>

<table>
<tr><td colspan="3">NCPC Online Courses</td></tr>
<tr><th>Course No.</th><th>Course Title</th><th>Description</th></tr>
<tr><td>AWR353</td><td>Using the Community Cyber Security Maturity Model (CCSMM) to Develop a Cyber Security Program</td><td>Using the Community Cyber Security Maturity Model to Develop a Cyber Security Program will introduce students to the DHS-supported Community Cyber Security Maturity Model (CCSMM) which can be used as a guide for communities and states in developing their own CCSMM-consistent cyber security programs. Students will learn what is required to develop a coordinated, sustained, and viable community cyber security program and resources available to assist in improving awareness, information sharing, policies, and plans.</td></tr>
<tr><td>AWR366</td><td>Developing a Cyber Security Annex for Incident Response</td><td>Cyber-attacks occur more frequently and have become increasingly sophisticated. Cybersecurity events now have the potential to significantly disrupt the business operations of government and critical infrastructure services. Public and private sectors, in the United States, are at increasing and continual risk of surprise attacks from nation-state and non-state actors. (Burgess, 2018)
The National Response Framework describes how preparedness can be achieved by developing an incident annex for each hazard. Incident annexes describe coordinating structures used to deliver core capabilities and support response missions unique to a specific type of incident.</td></tr>
</table>

		Incident annexes describe specialized response teams, resources, roles, responsibilities, and other scenario-specific considerations. At the end of this course, participants should possess the fundamentals needed to design and develop a cyber annex for states, locals, tribes, and/or territories (SLTTs). It addresses what the annex is, how it is used, who should participate in the design, implementation, and execution.