CYBERSECURITY ENGINEERING - CERTIFICATE

As the digital age advances, the need to protect the security, safety, and privacy of individuals and enterprises increases. This is true for a wide range of organizations — public, private, not-for-profit, and non-governmental — that all depend on cyber systems. As society becomes more and more connected and as smart systems continue to evolve, there is a clear need for engineers to develop a good understanding of cybersecurity principles.

The certificate in Cybersecurity Engineering provides students with the core concepts, tools and skills in cybersecurity engineering. These skills are essential for the design, integration, operation, and maintenance of large-scale systems in the government, military and civil industries. The cybersecurity engineering discipline is focused on the successful realization and protection of large-scale, interconnected systems. The scope of cybersecurity engineering spans the entire system lifecycle, from earliest conception through system retirement.

The College of Engineering offers the Cybersecurity Engineering certificate to prepare engineers with the knowledge they need to maintain a safe, technologically-enhanced environment.

This program is also approved for delivery via asynchronous or synchronous distance education technology.

Program Requirements

Code	Title	Semester Credit Hours
CYBR 601/ CSCE 701	Foundations of Cybersecurity	3
or CSCE 665	or Advanced Networking and Security	
ECEN 759/ CYBR 630	Hardware Security	3
Select two of the following:		6
CSCE 640	Quantum Algorithms	
CSCE 652	Software Reverse Engineering	
CSCE 665	Advanced Networking and Security	
CSCE 678/ ECEN 757	Distributed Systems and Cloud Computing	
CSCE 684	Professional Internship [2]	
CSCE 685	Directed Studies [2]	
CYBR 602	Law and Policy in Cybersecurity	
CYBR 603/ CSCE 703	Cybersecurity Risk	
CYBR 604/ CSCE 704	Data Analytics for Cybersecurity	
CYBR 660/ INTA 690	Cybersecurity Literacy for the Global Arena	
CYBR 661/ PSAA 608	Cybersecurity Policy, Issues and Operations - A Manager's Guide	
CYBR 684	Professional Internship [2]	
CYBR 685	Directed Studies [2]	
ECEN 604	Channel Coding for Communications Systems	
ECEN 647	Information Theory	
ECEN 684	Professional Internship [2]	
ECEN 685	Directed Studies [2]	
ECEN 753	Theory and Applications of Network Coding	
ECEN 758	Data Mining and Analysis	
ECEN 759/ CYBR 630	Hardware Security [1]	
ISTM 635	Business Information Security	
ISTM 645	IT Security Controls	
ISTM 655	Security Management and Compliance	
MATH 673/CSCE 673	Information, Secrecy and Authentication I	
Total Semester Credit Hours		**12**

[1] Course can be taken as a cybersecurity directed elective only if it is not taken as part of cybersecurity core.

[2] Course must be approved by the program director for inclusion in the certificate and include applications in cybersecurity engineering. The maximum number of hours allowable in 684 and 685 courses combined is 3.

Students may substitute courses not listed here for the cybersecurity directed elective with the approval of the certificate program director.