MASTER OF ENGINEERING IN THE FIELD OF CYBERSECURITY POLICY AND COMPLIANCE (STEM, ONLINE)

The online master of engineering (MEng) in cybersecurity policy and compliance degree program offers an engineering management-focused course of study, providing an overview of cryptography, security systems, algorithms, and software paradigms—a perfect choice for those interested in exploring the complex intersections between policy, business, and technology. Students in the program become familiar with industry-recognized frameworks and methodologies, preparing themselves to take charge in the fast-paced world of information security.

Students in the MEng in cybersecurity policy and compliance program graduate with the ability to:

- Implement appropriate forensic analyses of cyber incidents and use predictive analytics modeling to forecast cyberattacks.
- Devise and implement solutions that go beyond traditional IT practices to delineate specific and actionable cyber intelligence.
- Formulate short- and long-term cybersecurity strategies and policies for their enterprises by identifying compliance laws and applying industry best practices.
- Design an organization's mobility solution while integrating mobile device management with these practices.
- Manage threat vulnerabilities and exploits, designing and implementing cybersecurity situational awareness procedures for an organization to safeguard its sensitive data and sustain its fundamental operations.
- Face the future of information assurance with the creative, technical, and managerial skills that employers are seeking in government, intelligence, and security analysts and executives.

This is a STEM designated program.

- Visit the program website (https://online.engineering.gwu.edu/online-master-engineering-cybersecurity-policy-compliance/) for additional information
- Download a free brochure (https://online.engineering.gwu.edu/sites/g/files/zaxdzs5816/files/2024-03/me.cyberpolicy.2024.pdf)
- Begin your application (https://online.engineering.gwu.edu/apply/)

ADMISSIONS

Admission deadline:

Admission offered on a rolling basis for Fall, Spring, and Summer terms.

Prior academic records:

Transcripts are required from all colleges and universities attended, whether or not credit was earned, the program was completed, or the credit appears as transfer credit on another transcript. Unofficial transcripts from all colleges and universities attended should be uploaded to your online application. Official transcripts are required only of applicants who are offered admission.
Students with degrees from non-US universities should submit certified course-by-course and degree evaluations of their transcripts. For a list of accredited evaluation agencies, please click here (http://www.naces.org/members/). These agencies can translate and evaluate your transcripts by determining the equivalent course, grade, and degree in the United States.

Statement of purpose:

In no more than 250 words, describe how the Cybersecurity Policy and Compliance program fits into your professional life and career objectives.

International applicants only:

Please review International Applicant Information (http://graduate.admissions.gwu.edu/international-applicants/) carefully for details on required documents and English language requirements.

For more information on the admission process, please visit: the online program admissions web site (https://onlinecybersecurity.seas.gwu.edu/me-cybersecurity-policy-compliance/admissions/).

Contact for questions:

applyonline@gwu.edu - 1-833-330-1454 / Ext. 1 (phone) - 1-949-524-8638 (fax)
11:00am-7:30 pm, Monday through Friday

REQUIREMENTS

The following requirements must be fulfilled: 30 credits in required courses.

Code	Title	Credits
Required		
CSCI 6012	Cybersecurity and Privacy	
CSCI 6532	Information Policy	
EMSE 6540	Management of Information and Systems Security	
CSCI 6013	Security in Mobile Computing	
CSCI 6534	Information Security in Government	
ECE 6132	Secure Cloud Computing	
EMSE 6542	Cybersecurity Risk Management and Compliance	
EMSE 6543	Managing the Protection of Information Assets and Systems	
EMSE 6544	Auditing, Monitoring, and Intrusion Detection for Information Security Managers	
EMSE 6546	Cybercrime for Information Security Managers	