CYBERSECURITY POLICY & RISK MANAGEMENT (CPRM)

Course numbers with the # symbol included (e.g. #400) have not been taught in the last 3 years.

CPRM 710 - Foundations of Cybersecurity Policy
Credits: 4
Examine the societal and organizational impacts of cybersecurity policy in our interconnected world that is increasingly dependent on advanced technologies and systems for communications and control. Explore the components of information systems and control systems and review the history and development of cybersecurity. Gain an appreciation of policy as one tool for managing risk and start to consider the challenges of cybersecurity policy-making.

CPRM 720 - Policy Development and Communications
Credits: 4
Discover the fundamental concepts and practices for developing and drafting organizational policy, including related documents to support implementation. Explore how to communicate policies to internal and external audiences (in both written and oral communications). Learn how to incorporate organizational priorities and mandates into managerial policies. Case studies are primarily based in security studies, but other professional fields are welcomed.

CPRM 730 - Security Measures I
Credits: 4
This course introduces common technological and organizational measures for cybersecurity, with a focus on protection concepts. Students added the organizational impacts of security measures, and explore how best practices, standards, and organizational policy can help manage such measures. Topics include identity management, authentication, access control, data and system security and availability, encryption, integrity mechanisms, system maintenance, and continuity of operations. Note that we do not focus on how to technically implement these security measures.

CPRM 740 - Cybersecurity Standards, Regulations, and Laws
Credits: 4
We survey laws, regulations, and standards for cybersecurity in the United States, including "soft law" and self-regulation. Topics include the pros and cons of regulatory solutions and market solutions; the different approach to data protection regulation in the European Union; and cybersecurity concerns and regulatory authorities in various U.S. industries and sectors. Students become familiar with key standards bodies involve in cybersecurity, and explore organizational processes for remaining current with industry best practices.

CPRM 750 - Security Measures II
Credits: 4
This course continues surveying common technologies and organizational measures for cybersecurity, with a focus on detection and organizational relationships. Topics include auditing and log records; monitoring and testing for threat detection; vulnerability scans; and the security of external services (e.g., cloud providers) an supply chains. We do not focus on how to technically implement these measures. Students assess organizational impacts and explore how best practices and standards can help manage such measures.

CPRM 790 - Organizations, Change Management, and Leadership
Credits: 4
This course examines both private and public institutions as systems whose effectiveness depends on how an organization adapts to opportunities, threats, and demands (external and internal). Students explore the design and leadership of ethical and socially responsible organizations. In course examples and exercises, students will apply this knowledge to their respective research interests (e.g., cybersecurity, analytics, criminal justice, public health, etc.).