

Professional Studies Cybersecurity Risk Management (MPCR)

MPCR 5000 Ethics in Cybersecurity 3 Credits

In the first part of this course, students are introduced to methodologies, principles, values, and frameworks to facilitate the study of ethics. In the second part of the course, students study discipline- and field-specific codes of ethics within the profession. The course explores the ethical responsibilities all cybersecurity professionals have towards themselves, corporations, the government, and the public. Students contrast the roles and responsibilities of security professionals with those of other information technology professionals. In the third part of the course, students apply an appropriate decision-making framework and gain experience navigating ethical issues in decision-making. Course discussions center on issues involving privacy, confidentiality, and sensitive information. During the final project, students codify an individual code of ethics in relation to professional codes of conduct. Students must receive a grade of B or higher to graduate.

Level: Graduate, Undergraduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a major in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

MPCR 5600 Disruptive Tech Org Change 3 Credits

This course explores the impact of disruptive technological innovation on organizations and their ability to adapt to change. More precisely, students learn how to detect and anticipate disruptive technologies and their potential impact on organizational culture, processes, and strategies. The course places an emphasis on understanding organizational values, processes, resources, and migration capabilities. Upon completion of the course, students will be able to identify and apply sustainable solutions to accommodate disruptive innovations and capabilities to cope with organizational and industry changes.

Level: Graduate, Undergraduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a major in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

MPCR 5605 Security Architecture Design 3 Credits

This course introduces students to fundamental logical hardware, operating system, and software security components, and how to use those components to design, architect, and evaluate secure computer systems. Understanding these fundamental issues is critical to effective information security management. The course is divided into three sections. The first section covers the hardware and software required to have a secure computer system. The second section covers the 9 logical models required to keep the system secure. The third section covers evaluation models that quantify system security.

Level: Graduate, Undergraduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a major in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

MPCR 5610 Info Sec. Laws and Compliance 3 Credits

This course introduces students to privacy laws, regulations, and industry guidelines with significant security and privacy impact and requirements. The course primarily examines laws and regulations from the United States, but it also includes some coverage of international laws. The course is divided into four sections. First, students are exposed to broadly-applicable laws and regulations that address information security. Second, students receive an introduction to industry-specific guidelines and requirements (FISMA, NERC, HIPAA, HITECH, PSQIA3, etc.). Third, students examine key state laws and regulations that impact information security management (such as relevant laws in California, Massachusetts, and New York). Finally, students scrutinize other countries' laws and regulations related to information security and privacy (such as laws in Canada, Mexico, and the European Union) and international standards such as ISO 27001 and 27032.

Level: Graduate, Undergraduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a major in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

MPCR 5615 Comm Strat for Info Sec Profs 3 Credits

This course addresses several leadership considerations, including how to navigate culture and style practices within organizations. Students learn how to deploy continual reinforcement in their communications strategy, especially when addressing the issues of risk and change. The course examines multiple communication approaches as well as tools and techniques that are appropriate for different audiences. Finally, students learn how to plan and implement a workforce cybersecurity awareness communications campaign.

Level: Graduate, Undergraduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a major in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

MPCR 5620 Cybersec Governance Frmwrk 3 Credits

This course prepares students to develop governance frameworks for information security management. Students learn how to develop holistic and integrated frameworks that include: (1) strategic planning; (2) security architecture policy and standards; (3) cultural and organizational awareness, training, and change management principles; (4) security operations; and (5) compliance and audit support elements. Students will study existing frameworks that are recognized as best practice in the public and private sectors (federal government, critical infrastructure, ISO 27000 for commercial, etc.).

Level: Graduate, Undergraduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a major in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

MPCR 5661 Info Assurance Risk Mgmt 3 Credits

This course provides an overview of enterprise security, privacy and information security assessment and management, and cybersecurity.

This course concentrates on tangible and intangible costs and examines concepts of information assurance and security risk assessment. Students learn how to assess information security risks and develop solutions. Students also learn traditional risk treatment options (accept, avoid, remediate/reduce, transfer) and apply them to IA/cyber risk management. Topics covered include social engineering, risk assessment, recovery and response, enterprise security, and formal techniques and policies.

Level: Graduate, Undergraduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a major in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

MPCR 5750 Information Security 3 Credits

This course provides theoretical and applied foundations of information security and assurance. Students study various types of cyber-crime and vulnerabilities of government computer systems and information networks. Students learn about strategies for the protection of information and computer systems and how to mitigate and respond to breaches of those systems.

Level: Graduate, Undergraduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a major in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

MPCR 6656 Secure Cloud Computing Archit 3 Credits

This course explores the emergence of cloud computing and security architecture deployed to protect data. First, students are introduced to cloud computing, virtualization, legacy hardware and software considerations, approaches to transitioning information technology from legacy systems to a shared managed service model, and various cloud computing models (including private, public, hybrid, and community clouds). After being familiarized with cloud computing, students are introduced to various type of security architectures, standards, protocols, and services used in private and public sectors

Level: Graduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a major in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

Enrollment is limited to Graduate level students.

MPCR 6662 CryptographyNetwork Security 3 Credits

This fundamental course covers the theory of encryption and standard protocols for data communications and network security. Students will learn the goals of cryptography such as data privacy, authenticity and integrity. Topics that may be covered include PKI, digital signatures, message authentication codes, hash functions, etc. An examination of network security defenses and countermeasures are also covered.

Level: Graduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to Graduate level students.

MPCR 6705 Managing Cyber Incident Resp 3 Credits

This course teaches students the fundamental skills needed to handle and respond to computer security incidents in an information system. This course introduces various underlying principles and techniques for detecting and responding to current and emerging computer security threats. Students learn how to manage a variety of types of incidents, and various laws and policies related to incident response are also covered. The course covers three main types of incidents: data breaches, advanced malware, and targeted attacks. Students learn how to plan for, respond to, and report these incidents.

Level: Graduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a major in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

Enrollment is limited to Graduate level students.

MPCR 6710 Mobile Device App Security 3 Credits

This course prepares students to develop a mobile device security strategy by identifying the mobile threat models and creating mobile security policies that establish device enrollment procedures, define permissions on usage and control, enhance connectivity control, and specify acceptable use of mobile devices in a working environment. Students also learn how to evaluate mobile device vulnerabilities, establish mobile device management processes, and design procedures to protect specific technology such as iPhone, iPad, and Android devices (such as secure access solutions and credential safeguards). Finally, students learn how to implement mobile application security measures through the application development process.

Level: Graduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to Graduate level students.

MPCR 6715 Securing Digital Supply Chain 3 Credits

This course examines how organizations are increasing security of their supply chains for critical products, materials, and systems. Students will focus on digital threats and vulnerabilities. The course explores case examples and industry and government best practices related to mitigation tools, strategies, and protective measures of Supply Chain Risk Management (SCRM) programs.

Level: Graduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a major in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

Enrollment is limited to Graduate level students.

MPCR 6730 AI Security Data Privacy 3 Credits

This course offers a comprehensive overview of the essential practices of securing AI systems and protecting data. The first part of the course focuses on the security threats unique to AI, including adversarial attacks, data poisoning, and model theft. Students will learn about the techniques used to exploit AI systems and the strategies to defend against these threats. This includes best practices in securing AI data, algorithms, and infrastructures. The second part of the course examines the core concepts of privacy, including data confidentiality, integrity, and the rights of individuals regarding their personal information. Students will explore issues such as data surveillance, profiling, and the potential for AI to infringe on personal privacy. Students will learn about various scenarios where AI's data processing capabilities might conflict with privacy norms and expectations. Practical strategies for preserving privacy in AI systems form a key part of the curriculum. Students will explore techniques such as anonymization, data minimization, and secure data storage.

Level: Graduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a program in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

Enrollment is limited to Graduate level students.

Enrollment limited to students in the School of Continuing Studies college.

MPCR 6770 Cyber Defense Analysis 3 Credits

This course focuses on analyzing cyber defense for computing and network systems. The course exposes the students to the various cybersecurity tools and skills. Cybersecurity experts and actors can use some of these to exploit a network system.

Level: Graduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a major in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

MPCR 6775 Cyber Threat Intelligence 3 Credits

This course focuses on profiling adversaries in the cyber space (hackers, organized crime, insiders, foreign states) and analyzing techniques, tools and processes they are using to perpetrate attacks against critical assets. Students will be able to develop threat indicators, determine potential implications for existing information systems and exploitation systems, and formulate advice on how to neutralize threats or thwart possible attacks.

Level: Graduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a major in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

Enrollment is limited to Graduate level students.

MPCR 6780 Cyber Surv.OpLegal; Framework 3 Credits

Cyber Surveillance Operation & Legal Framework Cyber surveillance operations are indispensable to collect the information necessary to anticipate, discover, and investigate malicious activities on the Internet. This course prepares students to execute surveillance and counter-surveillance operations and learn about the different phases of cyber surveillance operations including planning, targeting, collecting, and terminating. Students will also study legal implications and apply diverse regulations to the conduct of cyber surveillance operations.

Level: Graduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a major in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

Enrollment is limited to Graduate level students.

MPCR 7990 Capstone 3 Credits

Program staff will manually register eligible students for capstone course. A grade of "B" or higher is needed to pass this course. Core requirement for MPS degree.

Level: Graduate

Grading: Main Campus (UGrad, Grad)

Course registration restrictions:

Enrollment is limited to students with a major in Cybersecurity Risk Management, Cybersecurity Risk Management, Cybersecurity Risk Management or Cybersecurity Risk Management.

Enrollment is limited to Graduate level students.

Enrollment limited to students in the School of Continuing Studies college.