UNIVERSITY of WASHINGTON | TACOMA

MASTER OF CYBERSECURITY AND LEADERSHIP (MCL) CURRICULUM GUIDE

THE MASTER OF CYBERSECURITY AND LEADERSHIP (MCL) is a non-thesis, forty (40) quarter credit-hour, cohort-based program. The curriculum is dually taught between faculty from the School of Engineering and Technology (SET) and the Milgard School of Business (MSB). The technically-oriented curriculum focuses on understanding the basic operations and functionality of cybersecurity systems and information assurance. This is complimented by a more behaviorally-oriented curriculum that emphasizes the management of technical professionals and organizational leadership.

Ten (10) required courses are offered sequentially over four consecutive academic quarters – or twelve (12) months. A Cybersecurity Technology course from SET and a Business course from MSB, are delivered concurrently over Summer, Autumn, Winter, and Spring Quarters. totaling eight (8) courses. Another two (2) required capstone courses are offered for both Winter and Spring Quarters. These courses set the foundation for completing the team-based capstone projects by the conclusion of the program.

SUMMER COURSES

T CSL 550 – 5 credits
Networking and Internet Security

Looks at the issues of information security with a focus on raising students' awareness of the difficulties of maintaining a secure network environment, and providing them with fundamental knowledge and skills to implement and manage appropriate security practices and controls in an organization's network. Covers concepts of encryption and network security, explores threats posed to internet-based systems, and assesses network vulnerabilities. Learn operating system attacks and countermeasures, application attacks and countermeasures, cryptographic applications as well as legal and ethical security practice.

T CSL 520 – 5 credits
Business Essentials

Effective approaches to information security management. Overview of the key concepts, tools, and technologies that are vital in today's challenging business environment. Communication, marketing, accounting, finance, business law, and ethics. Through discussions, exercises, and assignments, students gain experience in applying their knowledge to business situations and making business decisions. Emphasizes interpersonal, technical, and problem- solving skills.

AUTUMN COURSES

T CSL 510 – 5 credits
Principles of Cybersecurity

Examines concepts, elements, strategies, and skills related to the information assurance lifecycle – policies, practices, mechanisms, dissemination, and validation – that ensure the confidentiality, integrity, and availability of information and information systems. Analyzes information assurance planning process, including determination and organizational goals, the threat spectrum, risk, and legal and ethical issues. Through readings, lectures, and discussions with academic and industry professionals, labs and security response exercises, students develop proficiencies in cybersecurity principles.

T CSL 580 – 5 credits
Project Management

Builds the foundations for information technology services and project management. Focused on key aspects of commoditization of hardware (e.g., on-demand, utility computing, cloud computing), software (i.e., software-as-a-service model), and business processes. Introduces the IT product development and service delivery processes with sound management principles for on-budget and on-time, high quality projects that meet end users' needs. Review fundamentals and offer practical solutions for these challenges.

WINTER COURSES

T CSL 530 – 4 credits
Cyber Risk Management

Examines the concepts, processes, and skills related to risk management in information assurance, including assessment, analysis, and mitigation planning. Analyzes risk management process through structured approaches that facilitate information assurance decision-making. Utilizes quantitative software and qualitative methodologies as well as labs, lectures, and discussion. Students develop risk management competencies through completing and presenting risk assessments to industry professionals.

T CSL 540 – 4 credits
Leadership and Team Dynamics

Focuses on conceptual training and practices so students can analyze and diagnose individual, group and network dynamics, evaluate organizational structures and processes, determine strategic and tactical options as a manager, and engage in managerial actions that enhance individual, team, and organizational performances. Develops critical thinking, communication, collaboration, and leadership skills.

T CSL 591 – 2 credits
Master's Capstone Project I

Small teams collaborate with government and industry partners to develop valuable contribution for a capstone customer in cybersecurity and business operations. Students secure customers, define a project plan, and create a statement of work contract.

SPRING COURSES

T CSL 570 – 4 credits
Cyber Forensics and Security Management

Applies and combines information assurance concepts, processes, and skills to solve case studies from practitioner experiences and explore the role of policy in creating successful information assurance programs. Leading private, public, and government sector organizations present real cybersecurity/risk management projects impacting their enterprises. Teams perform cybersecurity assessments and evaluations, and complete and present written evaluations, and recommendations to organizational leaders.

T CSL 560 – 4 credits
Strategic Organization Change

Readings, cases, experiential exercises, and discussions will explore theories, concepts, tools, and techniques for aligning an organization's strategy to the environment and creating, leading, and managing change. Examines concepts, tools, and techniques for understanding change dynamics and how successful cyber leaders and change agents create, implement, and manage change. Investigates perspectives on strategic change, considers change methodologies, and explores best practices.

T CSL 592 – 2 credits
Master's Capstone Project II
Continuation of TCSL 591. Collaborate with regionally government and industry and develop valuable contribution for a capstone customer in cybersecurity and business operations. With a customer, student teams execute and deliver the project statement of work previously developed in Capstone I.