MANAGEMENT AND LEADERSHIP OF CYBERSECURITY (EMaCS-03-04)				
DEGREE PROGRAM:		Master in Computer Science for the Human-Centric and Sustainable Industry		
SEMESTER: Third	**TYPE:** Basic	**CREDITS:** 5 ECTS	**WORKLOAD:** 125 hours	**MENTORING:** 0,5 hours/week
LANGUAGE: English				

OBJECTIVES	
General	Develop a broad range of skills related to designing and implementing information security management systems, assessing risks, developing continuity plans, and ensuring continuous improvement in information and cybersecurity practices.

Specific	• Acquire knowledge, skills and values in the fields relevant to management and leadership of cybersecurity:
	  ○ Leadership and management of information and cybersecurity.
	  ○ Risk management as part of management.
	  ○ Preparedness, continuity management and recovery.
	  ○ Supply chain and contract management.
	  ○ Information and cybersecurity management system (ISMS).
	  ○ Training as part of management and governance.
	• Be well-equipped to take on leadership roles in managing and securing the organization's information assets.

SUSTAINABILITY

The course significantly contributes to sustainability through its focus on Supply Chain Management within the cybersecurity context. By addressing the intricacies of managing the supply chain, the curriculum emphasizes ethical standards and considerations related to sustainability. This approach ensures that cybersecurity practices align with environmental and social responsibility, contributing to a more sustainable and resilient organizational ecosystem.

RESILIENCE AND HUMAN-CENTRIC DEVELOPMENT

In terms of resilience and human-centric development, the program makes substantial contributions by cultivating strong Leadership and Management skills in the realm of information and cybersecurity. The emphasis on Training as part of Management and Governance underscores the importance of continuous learning and development, fostering a human-centric approach to cybersecurity challenges. Additionally, the incorporation of Business Continuity Management recognizes the human impact in planning for and recovering from cybersecurity incidents, ensuring a resilient and people-focused response to evolving threats. The course also highlights the ethical dimensions of Protecting Personal Data and Privacy, promoting principles that enhance the human-centric aspects of cybersecurity practices. Through Problem Framing and Reflecting on Ethical Outcomes, the curriculum instills a mindset that prioritizes the well-being of individuals and aligns with human-centric principles in the ever-evolving field of cybersecurity.

SUBJECT MATTER

- Information Security Management Systems.
- Information Security Risk Management.
- Processes, controls, and tools.
- Business Continuity Management.
- Measuring, auditing, and continuous improvement.

COMPETENCES

C1. AQUIRING DATA, INFORMATION AND DIGITAL CONTENT
C3. MANAGING AND EVALUATING DATA, INFORMATION AND DIGITAL CONTENT
C7. PROTECTING PERSONAL DATA AND PRIVACY
C8. PROTECTING HEALTH AND WELL-BEING
C9. REFLECTING ON ETHICAL OUTCOMES
C11. PROBLEM FRAMING

C15. MANAGING SYSTEMS and/or PROJECTS
C17. COMMUNICATING EFFECTIVELY

LEARNING OUTCOMES

Knowledge	• Know how to design an information security management system for the organization.
	• Know about the processes, controls, and personnel and supply chain-related issues related to managing and leading cybersecurity.
	• Know how to effectively assess risks to the cyber operating environment.
	• Know how to develop preparedness and continuity plans.
	• Know about the importance of:
	  ○ situational awareness, measurement, and audits for the organization's information and cybersecurity and business operations.
	  ○ continuous improvement for maintaining the management system.

Skills	• Be able to design an information security management system (ISMS) for the organization, which involves establishing policies, procedures, and controls to manage information and cybersecurity effectively. • Be aware of the importance of addressing personnel and supply chain-related issues, as these can have a significant impact on an organization's overall security posture. • Assess effectively of risks to the cyber operating environment. • Be able to develop preparedness and continuity plans to ensure the organization business can effectively respond to and recover from cybersecurity incidents. • Be able to recognize the significance of maintaining situational awareness, monitoring and measuring cybersecurity performance, and conducting regular audits. • Acquire the ability to appreciate the need for continuous improvement in information and cybersecurity practices. • Acquire the ability to organize and conduct cybersecurity table to exercises within the organization.
Attitudes/values	• Apply principles of social safety and security.

TEACHING METHODS

Lecture-based teaching, group work, group discussions, homework assignments, presentations, …

Method	Class Workload	Individual Workload	Total
Theoretical Sessions	20	8	28
Group work and discussions	10	18	28
Presentations	6	12	18
Homework	2	49	51
TOTAL	**38**	**87**	**125**

EVALUATION

Group work 30%
Homework assignments 50%
Presentations 20%

PRECONDITIONS

Fundamentals of Cybersecurity.

DEPARTMENT	School of ICT
LECTURERS	Pia Satopää
LITERATURE	To be defined later.