FUNDAMENTALS OF CYBERSECURITY (EMaCS-03-03)				
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	Basics of information and cybersecurity. Comprehensive understanding of information and cybersecurity, covering foundational knowledge, risk management, compliance, data protection, security culture, basic concepts, training, risk assessment, practice evaluation, employee awareness, training implementation, risk communication, and promoting security culture.
Specific	• Acquire knowledge, skills and values in the fields relevant to cybersecurity: o Operational and threat environment. o Impact and influence. o Competence and awareness. o Information security culture. o Information security policy, guidelines, models, frameworks. o Information classification. o Risk management and controls. o Auditing.

SUSTAINABILITY

The Fundamentals of Cybersecurity course plays a pivotal role in contributing to sustainability by providing students with a comprehensive understanding of information and cybersecurity principles. Covering foundational knowledge, risk management, compliance, and data protection, the course instills a strong foundation for sustainable cybersecurity practices. Students learn about the identification of protected assets, emphasizing the role of data classification in risk management. The significance of audits for evaluating an organization's adherence to security policies ensures compliance with regulatory requirements, contributing to the sustainability of secure business operations. The course promotes the importance of a security culture, fostering security-conscious behaviors and proactive approaches to information security. By equipping students to assess cybersecurity risks and implement training programs, the course empowers individuals to contribute actively to the sustainability of secure information environments.

RESILIENCE AND HUMAN-CENTRIC DEVELOPMENT

The Fundamentals of Cybersecurity course significantly contributes to resilience and human-centric development by enhancing students' knowledge, skills, and values in the cybersecurity domain. Students acquire the ability to assess an organization's level of competence in information security and implement training programs, fostering a resilient workforce. The emphasis on risk assessment and the evaluation of existing security practices prepares students to identify and address vulnerabilities, contributing to the resilience of organizational cybersecurity. The course instills attitudes and values that promote effective communication of findings to management and stakeholders, highlighting risks and proposing mitigation measures. By emphasizing the importance of a security culture, the course contributes to human-centric development, creating awareness and encouraging proactive approaches to information security that prioritize the well-being of individuals within the organizational context.

SUBJECT MATTER

- Cybersecurity concepts and terms.
- Information classification.
- Cyber threat reports and threat intelligence.
- Common software vulnerabilities and related taxonomies.
- Common network security protection techniques.
- Cryptography fundamentals.
- Public key infrastructure.

- Wireless communication security basics.

COMPETENCES

C3. MANAGING AND EVALUATING DATA, INFORMATION AND DIGITAL CONTENT
C6. USING MACHINE LEARNING AND A.I. TECHNIQUES
C7. PROTECTING PERSONAL DATA AND PRIVACY
C9. REFLECTING ON ETHICAL OUTCOMES
C11. PROBLEM FRAMING
C15. MANAGING SYSTEMS and/or PROJECTS
C16. WORKING WITH OTHERS

LEARNING OUTCOMES

Knowledge	• Know about fundamental principles, concepts, and terminology related to information and cybersecurity. • Know about the identification of protected assets as a key factor in risk management and knows the process of classification. • Know about the importance of audits and its role in evaluating an organization's adherence to security policies, procedures, and regulatory requirements for ensuring its compliance. • Know about the significance of: o information and cybersecurity for the organization's business operations data classification as a part of safeguarding organizational information. o a security culture for ensuring information security within the organization.
Skills	• Be able to understand the basic administrative and technical concepts of information and cybersecurity. • Be able to assess the organization's level of competence in information and cybersecurity and plan and implement training programs. • Be able to assess information and cybersecurity risks and report them to management. • Acquire ability to evaluate an organization's existing security practices and identifying areas that require improvement. • Be aware of the importance of information and cybersecurity for business operations and the importance of employee awareness and participation in maintaining a strong security culture. • Be able to create and implement training programs to educate employees about information and cybersecurity best practices. • Acquire ability to assess information and cybersecurity risks and report them to management.
Attitudes/values	• Be willing to communicate the findings effectively to management and another stakeholders, highlighting the risks and proposing appropriate mitigation measures Apply principles of social safety and security. • Promote the significance of a security culture which involves security-conscious behaviours of the need, creating awareness, and encouraging a proactive approach to information security.

TEACHING METHODS

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

Method	Class Workload	Individual Workload	Total
Theoretical Sessions	16	8	24
Group work and discussions	4	20	24
Presentations	6	20	26
Homework	2	49	51
TOTAL	**28**	**97**	**125**

EVALUATION	
Group work 30% Homework assignments 50% Presentations 20%	
PRECONDITIONS	
None	
DEPARTMENT	School of ICT
LECTURERS	Pia Satopää
LITERATURE	To be defined later.