VIDZEMES AUGSTSKOLA

FACULTY OF ENGINEERING
STUDY COURSE DESCRIPTION

Course Title:	**Cybersecurity Policy**				
Course code (LAIS):	**DatZ5015**				
Study programme:	**CYBERSECURITY ENGINEERING**				
Level of Study programme:	☐ 1st level professional higher education				
	☐ Professional Bachelor				
	☒ Professional Master				
	☐ PhD level				
Type of Study programme:	☐ Compulsory course (Part A)				
	☒ Professional specialization courses (Part B, compulsory)				
	☐ Professional specialization optional courses (Part B, optional)				
	☐ Elective courses (Part C)				
Course Workload:	**Credits**	**ECTS**	**Academic hours**	**Contact hours**	**Independent work hours**
	2	3	80	24	56
Course Author/ Tutor:	**Sintija Deruma**				
	Academic position scien./acad. degree				
	Consultation: according to the schedule for each semester				
Course Form:	Full time				
Study year, semester:	2019 /2020	2nd and 4th semesters			
Language:	Latvian				
Prerequisites for the Course:	Basic skills in developing regulations				
Course Summary:	The aim of the study course is to increase students' understanding of the cybersecurity and information security policy and its development principles.				
Course Methods:	Lectures, practical workshops, seminars, discussions, group work				
The Type of Final examination	Exam				
Requirements for Credits:	Practical work 60%, final exam 40%				

Course Contents:	Cybersecurity, information security policies and the basic principles of their development, incidents, violations and their investigation in the field of information security. Preventive measures to ensure information security and data protection, implementation of information security principles.	
Learning Outcomes	**Learning Outcomes**	**The evaluation methods and criteria**
	Knowledge	
	A student **knows and understands** the information security risks of an organization.	lectures, practical classes, seminars, discussions, group work
	Skills	
	A student is **able to apply** appropriate methods, security measures, security controls to implement information security system.	lectures, practical classes, seminars, discussions, group work
	Competency	
	A student is able to **analyse and evaluate** the information security risks, vulnerabilities, weaknesses in an organization, and provide recommendations for their elimination.	practical classes, seminars, discussions, group work
Course Compulsory literature:	Cybersecurity Policy handbook, Accellis https://accellis.com/wp-content/uploads/Cybersecurity-Policy-Handbook.pdf	
Course additional literature:	State of Cybersecurity, ISACA, 2017 https://cybersecurity.isaca.org/static-assets/documents/State-of-Cybersecurity-part-2-infographic_res_eng_0517.pdf	
Course approval date:	January 3, 2018	Course last revision date:

Study Course Plan:

Date*	Theme	Academic hours		Study Form
		contact lessons	Independent work hours	
	The policies of cybersecurity and information security and the basic	6		Lecture, situation analysis, discussions

	principles of their development, roles and responsibilities.			
	Incidents, violations and their prevention in the field of information security.	6		Lecture, situation analysis, discussions
	Preventive measures to ensure information security and data protection, implementation of information security principles in the policy development.	6	10	Lecture, situation analysis, discussions
	Practical work: security policy analysis, development seminar.	4	10	Lecture, situation analysis, discussions
	Development of a security policy.		36	Group work, practical assignments
		2		Final exam
	Hours total:	***24***	***56***	

** The date is specified before the implementation of the course*