VIDZEMES AUGSTSKOLA

FACULTY OF ENGINEERING
STUDY COURSE DESCRIPTION

Course Title:	**Security Culture**					
Course code (LAIS):	**MKI_003**					
Study programme:	**"Cybersecurity engineering"**					
Level of Study programme:	☐	1st level professional higher education				
	☐	Professional Bachelor				
	☒	Professional Master				
	☐	Academic 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:	**Egons Buss**					
	Academical position, scien./acad.degree					
	e-mail:					
	Consultation: according to the schedule for each semester					
Study Form:	Full time studies					
Study year, semester:	2019/2020, 4th semester					
Language:	Latvian, English					
Prerequisites for the Course:	Basic skills in human resource management An understanding of security management					
Course Summary:	The aim of the course is to widen the students' understanding of their employees' behaviours, habits and attitudes impact during the information security process					
Assessment:	Exam					
Requirements for Credits:	Practical work 60%, final examination 40%					
Abiding by the Academic Ethics	Students must abide by the academic and research ethics, Vidzeme University of Applied Sciences Ethics Regulations, incl.: – study papers must be independently developed; – the study work should reference all statements, ideas and data used that have been authored by someone else; – appropriate data acquisition methods should be used in the acquisition of data, the research ethics must be respected, empirical data must be collected independently and cannot be distorted or falsified; – the examination must be carried out by the student independently, without the use of supporting materials and/or consultations with other students, unless the lecturer states otherwise. In the event of non-compliance with the academic and research ethics, punishment is imposed in accordance with the ViA Ethics Regulations and the study course must be re-taken, unless the punishment is extramarital.					
Learning Outcomes; the evaluation methods and criteria	**Learning Outcomes**			**The evaluation methods and criteria**		
	Knowledge					
	The student knows and fully comprehends security culture and safety training necessity; people and the importance of their habits in the information security process			Lectures, practical tasks, seminars, discussions, group projects		
	Skills					
	The student is able to use the needed methods to invent, dynamically improve and tackle a long-term information security training programme			Lectures, practical tasks, seminars, discussions, group projects		

	Competency	
	The student can analyse and deliberate the results of the information safety training programmes, as well as improve and perfect its point	Practical tasks, seminars, discussions, group projects
Course Compulsory literature:	1) Kai Roer, Security Culture Framework https://securityculturеframework.net/ 2) LVS EN ISO/IEC 27001 standarts	
Course additional literature:	CSX Cybersecurity Fundamentals study book https://cybersecurity.isaca.org	
Course confirmation date:	3rd January 2018	
Date of course description update:		

Study Course Plan:

Date	Theme	Academic hours		Study Form/ Organization of independent work of students and task description
		Contact hours	**Independent work hours**	
The date is specified before the implementation of the course	Defining the organisation's safety culture. Safety standard, guideline and research analysis and every-day use.	**4**		Lecture, analysis of the situation, discussions
	The impact human factors have on information security and processes in an organisation.	**4**		
	Educational framework on the understanding of security, meeting quality demands, roles and responsibility.	4		Lecture, analysis of the situation, discussions
	Success and failure factors of safety training; different levels and difficulty of training; setting a target audience; tools and methods; effectivity measurement.	4		Lecture, analysis of the situation, discussions
	Information security training analysis, successes and mistakes; the planning of change in information security processes and improvement of training programmes.	2		
	Practical work: leading the safety training.	4		Lecture, analysis of the situation, discussions
			56	Group work, practical tasks
		2		Final examination
	Hours total:	***24***	***56***	