MEĐIMURJE POLYTECHNIC IN CAKOVEC

SYLLABUS COLLEGE

ACADEMIC YEAR:	2020./2021.

1. GENERAL INFORMATION ABOUT THE COLLEGE

1.1. Course name	BUSINESS SECURITY MANAGEMENT			
1.2. Study programme(s)	Undergraduate professional studies *Management of tourism and sport*			
1.3. Course status (O,E)	electoral	**1.6. Method of teaching (number of hours)**	**Lectures**	30
1.4. Course code			**Exercise**	15
1.5. Acronis of the course	BSM		**Seminar**	
1.6. Semester	V.		**E-learning**	
1.7. Points value (ECTS)	5	**1.7. Place and time of teaching**	Rooms of međimurje polytechnic in Cakovec, according to the schedule published on the website.	

2. TEACHING STAFF

2.1. Holder/i-vocation	mr.sc. Miljenko Vrbanec, senior lecturer	**Contact**	mvrbanec@mev.hr
		Contact	
2nd 2nd In TheHague. Assistant/i-vocation		**Contact**	
		Contact	
2.3. Contractor(s)		**Contact**	
		Contact	

3. COURSE DESCRIPTION

3.1. Objectives of the college	The aim of the college is to adopt basic knowledge of forms of security threats in the field of business security in the state, private and public sectors, on the organization of business security in businesses and institutions, global security trends, ways of protecting business information and data sources. Students will learn to draw up a safety plan in businesses and institutions.
3.2. Conditions for admission and passing of the course	Required incoming to lectures and exercises.
3.3. Learning outcomes	The student is expected to take the job security course after the course. 1. andidentify threats in the field of business security 2. present the purpose and objective of business security in businesses and institutions 3. identify steps and methods in developing a company safety plan 4. analyse the role of business security in the success of 5. present a legal framework in the field of business security
3.4. Content of the course	The college deals with basic concepts in the field of business security in companies and institutions. Global security trends and ways to protect business information, data sources are presented. Show up in analytical methods, business intelligence, the role of management and employees in the field of business security, the protection of the material and intangible assets of the company. In addition, it will expose the functioning of crisis situations,

		the role of the media in undermining the public's business reputation and how to develop a security plan in businesses and institutions.							
3.5. Types of teaching	X	Lectures	X	Exercise		Mixed e-learning	X	Stand-alone tasks		Laboratory
		Seminars and workshops		Distance education		Field training		Multimedia & Network		Mentoring work
		Rest:								

3.6. Performance language	Croatian

3.7. Monitoring of student performance (enter the number of ECTS points for each activity so that the total number of ECTS points corresponds to the points value of the course)	2.00	Attendance	0,25	Seminar work		Essay
	0,25	Activity in Class		Project		Referat
	1.00	Colloquium		Practical work		Continuous knowledge verification
	1.00	Written exam		Experimental work		
	1,50	Oral exam		Research		

3.8. Evaluation and evaluation of students' work during class and on the final exam

Activity Specification	Percentage %	Score
Evaluation during class		
Presence in class	5%	5
Activity in Class	5%	5
Seminar work/ project/ essay	20%	20
Colloquium 1	35%	35
Colloquium 2	35%	35
Evaluation of exam work for students who did not co-late		
Written exam	*70%*	*70*
Oral exam	*30%*	*30*
Total:	**100%**	**100**

Written exam
The written exam is passed through two colloquials or through a written exam.
Oral exam
A student in an oral exam is entitled to the public. An assistant or another student must be present in the room. Test questions must be written to determine whether all outcomes have been verified. The oral exam is mainly used as an upgrade to be written, only exceptionally as the only form of knowledge verification.

3.9. Evaluation criteria – elaboration by outcomes

	How the outcome is laid					
	Attendance	Activity in Class	Colloquium 1	Colloquium 2	Seminar	Total
Outcome 1			15			15, 2014 in New York
Outcome 2			15			15
Outcome 3				15		15
Outcome 4				15		15
Outcome 5				15		15

Beyond the outcome	5	5			15	25
Total	**5**	**5**	**30**	**45**	**15**	**100**

Scoring the outcome (in order to pass the colloquium/exam the student must achieve at least 50% of the points for each learning outcome)
Points Rating
89 – 100 Excellent (5)
76 – 88 Very Good (4)
63 – 75 Good (3)
50 – 62 Sufficient (2)
 0 – 49 Insufficient (1)

3.10. Specifics related to the passing of the course	If the student collects 50% of the points of each outcome, he or she will have access to the oral exam directly. If a student does not achieve a sufficient number of points on the intermediate exam, they cannot access the next intermediate exam. Once points are scored in inter-exams for each learning outcome, they are no longer deleted. The student cannot access the exam period unless he or she has submitted a seminar paper. Seminar work is submitted within the agreed deadline, and certainly before the test period. The final assessment is obtained on the oral part of the exam.
3.11. Student obligations	Regular students are required to attend at least 70% of the total number of hours of lectures and exercises in order to exercise the right to take the exam. Outstanding students are required to attend at least 30% of the total number of hours of lectures and exercises in order to exercise. If the student has not fulfilled all the obligations provided for in the course, he or she is obliged to re-attend the lectures and to meet the requirements for joining the exam. Incoming can be compensated by online consultations, organized webinars and added tasks set by teachers. One class lasts 45 minutes and several hours make up the unit. Absence from one unit counts as one absence. Delays and excuses are recorded separately. In such a case, the student has missed more than 50% of the teaching and has a legitimate reason/apology, should submit a request to the Council of Departments, which then decides on the justification of student absences with the mandatory opinion of the course holder.
3.12. Written works	Seminar papers must be written by computer and must have a maximum of 12 text cards (TimesNew Roman, font of letters 12) (determined depending on ECTS points) from introduction to conclusion, together with images, table *attachments,* etc. Seminar papers must have an adequate front page, content, tagged pages and literature. The seminar paper should be divided into chapters and contained in addition to the literature list and a list of images and tables and graphs and finally a summary/conclusion in the size of 250 words. The student, with his signature, guarantees the authenticity of the work.

3.13. Mandatory literature	1.	Ivandić Vidović, D. Karlovic, L. Ostojic, A. : Corporate Security, Association of Croatian Security Managers, Zagreb, 2013.
	2.	Sučević, D. : Crisis management, Lider press d.d., Zagreb, 2010.
3.14. Supplementary literature	1.	Data Secrecy Act OG 79/07, 86/12
	2.	Information Security Act OG 79/07
	3.	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to

		the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)
	4.	Professional and scientific articles in the field of business security

4. ADDITIONAL INFORMATION ON THE COLLEGE

4.1. Quality check	The quality of the program, the teaching process, the teaching skills and the level of adoption of the building will be established by carrying out a written evaluation based on questionnaires, and in other standardized ways and in accordance with the acts of međimurje polytechnic in Cakovec.
4.2. Contacting the teacher	Students can contacted teacher during the consultation period and during class, while for brief questions and explanations can be contacted on any day during business hours by coming in person. It is possible to ask questions and e-mail to which it will be discussed in 48 hours at the latest. It is desirable that students for all ambiguities come as often as possible for consultations.
4.3. Course information	It is the obligation of each student to be regularly informed of the course. All maintenance or delay notices will be reported on the bulletin board and on the Polytechnic's website at least 24 hours in advance.
4.4. Contribution of the college to the study programme	Present information, ideas, problems and solutions to the professional and general public. Critically evaluate arguments, assumptions and data in order to create opinions and contribute to a solution to the problem. Make business decisions taking into account economic, environmental, legal and ethical norms.

5. ELABORATION OF THEMATIC UNITS (the number of elaborate hours is equivalent to the number of lectures and courses)

Lectures				
Hours	**Topic and description of the lecture**	**Method of operation** • direct teaching (presentation, instruction, pp presentation) • Learning by discovery (independent, guided, debate, debate) • Group/Collaborative Learning • case study • field teaching...	**Teaching outcomes**	**Learning outcome of the course**
1.	Defining the conceptof business security and legal sources.	Presentation, PP presentation.	Distinguish between legal sources and explain the general legal termse.	I1
2.	The concept and types of security threats in the private and public sectors in the field of business security.	Presentation, PP presentation.	Comment on the types of threats in the field of business security and explain the difference between the private and public sectors.	I1
3.	Pojmovalso in the field of business security: security trends, data sources, analytical methods, business intelligence, industrial espionage.	Presentation, PP presentation.	Present the main concepts in business security of the company.	I1

4.	The data collectionprocess.	Presentation, PP presentation.	Distinguish between legal and illegal sources.	I1
5.	Intelligence activity in the business of the company.	Presentation, PP presentation.	Analyze the business of companies in the field of collection, processing and distribution of business information.	I2
6.	Industrial espionage as a form of illegal collection of business information and data in the business of the company.	Presentation, PP presentation.	Explain the forms and ways of illegal data collection.	I2
7.	Protection of tangible and intangible assets of enterprises in the field of business security.	Presentation, PP presentation.	Present types of protection of tangible and intangible assets of the company.	I2
8.	The main features of Business intelligence in the business environment.	Presentation, PP presentation.	Interpret the main characteristics of business intelligenac in the business of the company.	I3
9.	The role of the media in ruining the public's reputation.	Presentation, PP presentation.	Analyze the role of the media in the context of business security.	I3
10.	Functioning of business organization in crisis situations.	Presentation, PP presentation.	Analyze crisis situations in the business environment.	I3
11.	Term and sources of normative regulations in the field of business security.	Presentation, PP presentation.	Distinguish sources of normative regulations in the field of business security.	I4
12.	Business security plan for businesses and institutions.	Presentation, PP presentation.	Present a safety plan..	I5
13.	Information security measures and standards.	Presentation, PP presentation.	Alsoanalyse information security measures and standards.	I5
14.	Use methods and tools to collect, process and analyze business information.	Presentation, PP presentation.	Explain the process of collecting, processing and analysing business information.	I5
15.	The impact of global, regional and national security on economic processes in the business environment.	Presentation, PP presentation.	Explain the functioning of the business security system under different influences.	I4
EXERCISES/ SEMINARS				

Hours	Topic and description of the lecture	Method of operation • direct teaching (presentation, instruction, pp presentation) • Learning by discovery (independent, guided, debate, debate) • Group/Collaborative Learning • case study • field teaching...	Teaching outcomes	Learning outcome of the course
1.	View legal sources in the field of business security	Learning by discovery.	Compare legal sources of varying rank.	I1
2.	Task	Group learning	Use methods of information analysis.	I1
3.	View standard evaluation analyses of information evaluations.	Learning by discovery.	Use methods of analysis.	I1
4.	View the distribution of business information within the company.	Learning by discovery.	Comment on the distribution.	I1
5.	Task	Group learning.	Analyze the role of protected data.	I2
6.	An example of creating a classified document.	Learning by discovery.	Comment on the production of the classified document and its declassification.	I2
7.	And the air of the Plan of Measures to Protect the Business Process.	Group learning.	Compare multiple forms of plans.	I2
8.	I. COLLOQUIUM	Independently.	Verification of outcomes I1,I2.	I1,I2
9.	Examples of intellectual property and its protection.	Learning by discovery.	Analyze the intellectual property protection process.	I3
10.	An exampleand a type of trade secrets.	Learning by discovery.	Critically, he's judging what's considered a trade secret.	I3
11.	View examples of marking classified documents.	Group learning.	Analyze the essential elements of business document tagging.	I4
12.	View the main features of a purchase agreement for example.	Learning by discovery.	Comment on the example of a purchase agreement.	I5
13.	View examples of business security crimes.	Learning by discovery.	Analyse examples of business security crimes.	I5
14.	View examples of crisis communication.	Learning by discovery.	Compare types of communication by event format.	I5
15.	II. COLLOQUIUM	Independently.	Verification of outcomes I3,I4,I5 .	I3,I4,I5