SYLLABUS

Basic information of the course	
University:	**University "Ukshin Hoti" - Prizren**
Academic unit:	**Faculty of Computer Science**
Study program:	**Information Technologies and Telecommunication**
Course:	**Security in IT networks**
Study level:	**Bachelor**
Course status:	**Mandatory**
Study year:	**3**
Number of hours per week:	**2+2**
Credit value - ECTS:	**6**
Time / location:	**It will be published in the university web site!**
Lecturers:	**Assoc. Prof. Dr. Naim Baftiu** **Ass. Betim Maloku, Ph. D. c.**
Contact details:	**naim.baftiu@uni-prizren.com** **betim.maloku@uni-prizren.com**
Course description:	The course provides basic concepts about data security and information technology systems, methods of security risks, operating system security and network security, cyber security etc.
Course objectives:	The aim of this course is to explain to students the basic concepts, definitions and best practices of data security and Information Technology Systems in general. The course begins with definitions on data and information, databases as well as basic concepts of data security. The elaboration of the attacks on the data and the way of protection from these attacks is done. Cryptography and data encryption forms also play an important role. Forms of data protection are explored in databases, software applications, computer network, servers and web servers, e-mail, etc. Students are explained how to retrieve data in the event of a data capture accident by hackers or damage to Information Technology systems.
Learning outcomes:	At the end of this course the student will be able to: - Know and understand the basics and basic notions of Data Security

	- Know and understand the terms of cryptography and the basic meanings of symmetric and asymmetric cryptography - Understand encryption algorithms and their types - Know the application of cryptography for data protection - Know the security concepts at the computer level - Know the security concepts of servers - Know the concepts of security at the level of computer networks - Know Internet security and Internet technologies - Recognize security risks - Knows security applications (software) - Knows issues of data protection planning and storage.

Contribution on student load (must correspond with learning outcomes)			
Activity	**Hours**	**Days/week**	**Total/hours**
Lectures	2	15	30
Exercise theoretical/laboratory	2	15	30
Practice work	1	2	2
Contact with lecturer/consultations	1	5	5
Field exercises	1	1	1
Midterms	2	2	4
Laboratory exercises	2	2	4
Individual time spent studying (at the library or home)	3	10	30
Final preparation for the exam	5	6	30
Time spent in evaluation (tests, quiz, final exam)	2	3	6
Projects, presentations, etc.	4	2	8
Total			**150**
Notice: 1 ECTS credits = 25 hours commitment, e.g. if the course has 6 ECTS credits student must have 150 hours during the semester.			

Teaching methods:	The course is a combination of lectures, discussions, numerical and laboratory exercises, while the assignments are presented by the laboratory course lecturers!
Assessment methods:	- Attendance in lectures and exercises: 5% + 5%.

	- Semestral project: 15%. - Midterm 1: 35%. - Midterm 2: 40%. - Or final exam: 100%.	
Assessment and grading:	**Vlerësimi në %**	**Nota përfundimtare**
	91% - 100%	10
	81% - 90%	9
	71% - 80%	8
	61% - 70%	7
	51% - 60%	6
	0% - 50%	5
Literature		
Basic literature:	1. Security in Computing, Fifth Edition, Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies.	
Additional literature:	1. Cryptography and Network Security, Principles and Practice, 5th Edition, William Stallings, Pearson Education, 2011. 2. Principles of Computer Security: CompTIA Security+™ and Beyond, Lab Manual, Second Edition,Vincent Nestler, Wm. Arthur Conklin,Gregory White,Matthew Hirsch. 3. Network Security Fundamentals, Eric Cole, Ronald L. Krutz, James W. Conley, Brian Reisman, Mitch Ruebush, and Dieter Gollmann Computer Security Fundamentals, Chuck Easttom, 2012 by Pearson.	
Study plan		
Week	**Lectures**	
First week:	• Introduction to course organization - syllabus (about lectures). • Introduction of the syllabus and topics that will be taught for the course Data Security. • Presentation of basic literature and supplementary literature. • Introducing the way of constructing the grade. Concepts of data security and information technology systems. • The importance of data security as part of computer security and computer network. • Characteristics of interventions in computer systems	
Second week:	• METHODS OF SECURITY RISKS	

	• Malicious code: Malware • Viruses, Trojans, logic bombs, worms • Other malicious code: web viruses • Secrets, "Rootkits", interface illusions, keystroke logging • Non-malicious flaws, Camouflaged channels • An side channels
Third week:	• OPERATING SYSTEM SECURITY • Controls for security flaws in programs • Stages of the software development cycle • Operating Systems Protection • Ja Separation against shared use Segmentation and calling.
Fourth week:	• OPERATING SYSTEM SECURITY II • User authentication • Verification factors • Passwords– Password attacks • Security policies and models
Fifth week:	• NETWORK SECURITY • Reliable design of operating systems • Design elements • Security features • Network security • Cyber Security
Sixth week:	• SERVER SECURITY • Network security • Server security and the role of servers in network security • Threats to networks
Seventh week:	• CRYPTOGRAPHY APPLICATIONS FOR INTERNET SECURITY • Basics of cryptography • Symmetric cryptography
Eighth week:	• First midterm.
Ninth week:	• CRYPTOGRAPHY APPLICATIONS IN VPN AND WIRELESS NETWORKS • Security controls through cryptography • Link layer security: WEP, WPA, WPA2
Tenth week:	• INTERNET SECURITY AND PRIVACY • Application of encryption in e-mail security • Internet Protocol Security Application (IPsec)
Eleventh week:	• COMPUTER AND NETWORK DATABASE PROTECTION SOFTWARE • Database security

	• Security requirements • Integrity, Audit, access control and availability
Twelfth week:	• RECOVERY FROM DESTRUCTION AND DATA STORAGE STRATEGIES • Security administration • Security planning (Disaster recovery)
Thirteenth week:	• PHYSICAL SECURITY • Legal and ethical issues • Intellectual property
Fourteenth week:	• Administrative security in the company.
Fifteenth week:	• Second (final) midterm.

Exercises

Study plan	
Java	**Exercises**
First week:	• Introduction to course organization – syllabus (about exercises). • Exercises from basic safety concepts
Second week:	• Exercises from safety hazards
Third week:	• Exercises from operating system security.
Fourth week:	• Exercises from operating system security.
Fifth week:	• Network security exercises.
Sixth week:	• Exercises from server security.
Seventh week:	• Exercises from cryptography for Internet security
Eighth week:	• Consultations about midterm 1.
Ninth week:	• Exercises from cryptography in VPN and wireless networks.
Tenth week:	• Exercises from Internet Security and Privacy.
Eleventh week:	• Database protection exercises.
Twelfth week:	• Exercises from recovery from destruction.
Thirteenth week:	• Exercises from physical safety
Fourteenth week:	• Administrative security in the company.
Fifteenth week:	• Consultation about midterm 2.

Academic policies and rules of conduct
• Generally lecture presentations will be made through MS PowerPoint, tables, material usage, computer programs and numeric exercises. • Additional resources (scientific papers, publications, national bulletins, as well as recent discoveries and research) will be provided by professors. • In the absence of the opportunity for practical work to be organized weekly, in cooperation with the management of the university, this activity will be organized on certain days in: organizations, companies, etc.

- During each session will be organized the conversation and co-participation with the students!
- Students are required to be regular in lectures and exercises!
- It will be evaluated when the students collaborate and participate in the lectures and course exercises!
- Timely arrival in lectures and exercises is mandatory!