Basic data of the subject	
Academic unit:	**Faculty of Engineering and Informatics** **Applied Informatics**
Title of the subject:	**IT Security**
Level:	**Bachelor**
Course Status:	**Obligatory**
Year of studies:	**II**
Number of hours per week:	**3**
Value of Credits - ECTS:	**5**
Time / location:	
Course lecturer:	**Prof.Ass.Dr.Dhuratë Hyseni**
Contact details:	Dhurate.hyseni@ushaf.net
Course Description:	*This course enables students to understand the connection the forms of attacks, algorithms for encryption/decryption, protocols for sending data in secure way through network, Firewalls, Viruses/Trojans, Wireless Security and IPsec.*
Objectives of the course:	*The module provides a basic approach to the field of IT security as well as problems and issues related to the security of IT systems.*
Expected learning outcomes:	*Upon successful completion of this course, student will be able to:* • *Enumerate the protective objectives of IT security* • *Enumerate Methods how the protection objectives can be ensured* • *Establish the identity and access management in web applications (system hardening)* • *Map security issues from web to cloud applications* • *Administrate security systems*

Contribution to the student load (which must correspond with learning outcomes)			
Activity	**Hour**	**Day/Week**	**In total**
Lectures with numerical exercises	3	15	45
Internship			
Contacts with teacher / consultations			
Field exercises			
Midterm, seminars and projects.	3	2	6
Homework			
Self-learning time student (at the library or at home)	3	15	45
Final preparation for the exam	7	2	14
Time spent on evaluation (tests, quiz and final exam)			
Projects and presentations.	3	5	15
Total			**125**

Teaching methodology:	*The course takes 15 weeks with 2 hours of lectures and 2 hours weekly individual and group exercises.* *Exercises will be held in the form of individual and group work in which concrete examples will be discussed.* *Active participation is extremely important so students are encouraged to attend lectures and exercises regularly and contribute to the discussions that take place in lectures. Lectures, exercise, individual work, discussions and group work.*
Assessment methods:	*Final Exam 50%* *Course work 50%*
The ratio of theory and practice:	*70% theory with exercises and 30% laboratory work.*
Literature	
Basic Literature:	1. *Conklin A. White G .: Principles of Computer Security. Mc Graw Hill, 2nd edition, 2010*
Additional Literature:	2. *Stallings W., Brown, L .: Computer Security Principles and Practice- Pearson, 2012*
Designed learning plan	
Week:	**Lectures and exercises to be held**
Week one:	*Introduction to Computer Security.*
Week two:	*Cryptography.*
Week three:	*Cryptography (continued)*
Week four:	*Authentication & Authorization.*
Week five:	*Security threads.*
Week six:	*First evaluation*
Week seven:	*Secure communication protocols.*
Week eight:	*Firewalls and Intrusion Detection Systems.*
Week nine:	*Business Continuity.*
Week ten:	*Disaster Recovery.*
Week eleven:	*Risk assessment.*
Week twelve:	*Web Application Security Identity.*
Week thirteen:	*Access Management Security.*
Week fourteen:	*Safety in the Web Management of security systems hardening Cloud Security.*
Week fifteen:	*Second evaluation*
Academic policies and rules of conduct	
Regular attendance of lectures and exercises is necessary, as well as active participation with discussion and solution of tasks. Not impeding the progress required for learning using mobile phones turned off or in silent mode.	