Course Name	Code	Term	Theory (hours/week)	Application (hours/week)	Laboratory (hours/week)	ECTS
Informatics Ethics	SBF130	2. Semester/ Fall	1	-	-	2
Prequisites	-					
Course language	Turkish					
Course type	Elective					
Learning and teaching strategies	Lecture, Question - Answer, Discussion, homework					
Instructor (s)						
Course objective(Aim of course)	The main aim of the course is to improve the level of concept knowledge and practical implementation skills on generating solutions to current problems of informatics ethics and IT security.					
Learning outcomes	1-To explain technological and pedagogical knowledge for problems related to computer security and informatics ethics. 2- To generate solutions for social conflicts of the information age. 3- To explain ethical theories in computer education. 4- To develop strategies for ethics education of the next generation.					
References	• Barger, R. N. (2008). Computer ethics: A case-based approach. New York, NY: Cambridge University Press. • Mason, R. O. (1986). Four ethical issues of information age. MIS Quarterly, 10,(1), 5-12. • Bynum, T. (2001). Computer ethics: Its birth and its future. Ethics and Information Technology, 3(2), 109–112. • Kert, S.-B., Uz, C., & Gecü, Z. (2014). Effectiveness of an Electronic Performance Support System on Computer Ethics and Ethical Decision-Making Education. Educational Technology & Society, 17 (3), 320–331.					

Course outline weekly:

Weeks	Topics
1. Week	Introduction to course
2. Week	Ethics as a concept, ethical theory, basic philosophical approaches, the relationship among ethics, morality and law. Ethical practices in social life. Professional ethics.
3. Week	Informatics ethics as an ethical branch, history of informatics ethics.
4. Week	The importance of individual responsibilities in the context of using application in digital setting.
5. Week	Four ethical issues of Information age
6. Week	The case samples used for informatics ethics education.
7. Week	The steps of process towards solving ethical issues.
8. Week	**MİDTERM EXAM**
9. Week	Personal and instutional data security management; informatics legislation and law.
10. Week	Basic concepts of cyber space and cyber security
11. Week	Cyber actors and attack methods
12. Week	Cyber defense methods.
13. Week	Security and ethics in mobile and social media environments, network security
14. Week	Security and ethics in mobile and social media environments, network security
15. Week	Security and ethics in mobile and social media environments, network security

ECTS (Student Work Load Table)

Activities	**Number**	**Duration**	**Total Work Load**
Course Duration (X14)	14	1	14
Laboratory			
Practice			
Field Study			
Study Time Of Outside Of Class (Pre-Study, Practice, Etc.)	14	1	14
Presentations (Video shoot/Poster preparation/Oral presentation, Etc.)			
Seminars	14	1	14
Project			
Case study			
Role playing, Dramatization			
Writing articles, Critique			
Time To Prepare For Midterm Exam	1	2	2
Final Exam Preparation Time	1	4	4
Total Work Load (hour) / 25(s)	48 / 25 = 1.92		
ECTS	2		

Evaluation System

Mid-Term Studies	**Number**	**Contribution**
Midterm exams	1	%100
Quiz		
Laboratory		
Practice		
Field Study		
Course Internship (If There Is)		
Homework's		
Presentation and Seminar		
Project		
Other evaluation methods		
Total Time To Activities For Midterm		100
Final works		
Final	1	%100
Homework		
Practice		
Laboratory		
Total Time To Activities For Midterm		100
Contribution Of Midterm Studies On Grades		%40
Contribution Of Final Exam On Grades		%60
Total		100

The relationship between learning outcomes and the program outcomes of the courses

This course is suitable for all programs within the scope of the Faculty of Health Sciences. Therefore, the level of contribution to the program outcomess is not specified.