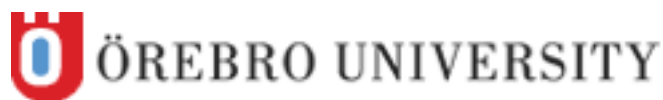

This course syllabus is discontinued or replaced by a new course syllabus.



Course Syllabus

Örebro University School of Business

Informatics, Social Aspects of Information Security, Second Cycle, 7.5 Credits

Course Code:	IK403A	Subject Area:	Field of Technology
Main Field of Study:	Informatics	Credits:	7.5
		Subject Group (SCB):	Informatics/Computer and Systems Sciences
Education Cycle:	Second Cycle	Progression:	A1N
Established:	2017-11-17	Last Approved:	2018-03-27
Valid from:	Autumn semester 2018	Approved by:	Head of School

Aims and Objectives

General aims for second cycle education

Second-cycle courses and study programmes shall involve the acquisition of specialist knowledge, competence and skills in relation to first-cycle courses and study programmes, and in addition to the requirements for first-cycle courses and study programmes shall

- further develop the ability of students to integrate and make autonomous use of their knowledge
- develop the students' ability to deal with complex phenomena, issues and situations, and
- develop the students' potential for professional activities that demand considerable autonomy, or for research and development work.

(Higher Education Act, Chapter 1, Section 9)

Course Objectives

1. Understand existing threats related to employees' poor information security behaviour, through analysing media reports of interest at the present time.
2. Understand the social aspects that affect employees' information security behaviour, based on contemporary research.
3. Understand which methods/tools that exist to change employees' information security behaviour, based on contemporary research.
4. Suggest appropriate ways of working with changing employees' information security behaviour, based on contemporary information security threats and existing methods/tools.
5. Have the ability to search for relevant and current information about information security.

Main Content of the Course

The course contains four modules:

1. Analysis of threats and incidents related to employees' information security behaviour reported in media. During this module we introduce threats related to employees' poor information security behaviour. These threats are introduced using a case on one or more incidents that act as a catalyst for students' search for additional cases in media. (Addressing goals 1 and 5)
2. Theoretical models about social aspects that have an impact on employees' information security behaviour. During this module the students read provided course literature, and watch recorded lectures. The students also attend seminars where they receive a case and discuss how different

models can explain the behaviour. Social aspect is used as an umbrella term for concepts, such as, culture, values, value conflicts, punishment, neutralisation, ethics, loyalty, and appetite of risk. (Addressing goal 2)

3. Methods and tools to change employees' information security behaviour. During this module the students read provided course literature, and watch recorded lectures. The students also attend seminars where they discuss how a provided awareness programme fits with an existing organisational culture. (Addressing goal 3)

4. Assessing and choosing a way of working to change employees' information security behaviour. The students work with cases where they suggest appropriate ways of working with changing employees' information security behaviour. (Addressing goal 4)

Teaching Methods

The employed teaching methods are anchored in flipped classroom and case-based learning. Flipped classroom means focusing on exploring topics in greater depth and creating meaningful learning opportunities in class time, while content delivery is made outside of the classroom. Case-based learning means that scenarios from real-world examples are used to as a point of departure for in class activities and assignments.

In this course these teaching methods are implemented through online lectures, individual readings, in-class activities based on cases, and group assignments based on cases.

Students who have been admitted to and registered on a course have the right to receive tuition and/or supervision for the duration of the time period specified for the particular course to which they were accepted (see, the university's admission regulations (in Swedish)). After that, the right to receive tuition and/or supervision expires.

Examination Methods

Analysis of Currently Reported Threats and Incidents, 1.5 Credits. (Code: 0110)

Group assignment to analyse threats and incidents reported in media. Seminar where cross groups are created. These groups discuss the results from each individual group's analysis of threats and incidents reported in media. The students have to give an account for their analysis. (Assesses goals 1 and 5).

Social Aspects, 1.5 Credits. (Code: 0120)

Seminars where the students, based on course literature and a provided case, have to identify social aspects that shape employees' information security behaviour. (Assesses goal 2).

Written Assignment - in Group, 2.5 Credits. (Code: 0130)

Group assignment where the students, based on a case, have to propose and argue for a way of working to change employees' information security behaviour. Provided arguments should be anchored in literature. (Assesses goals 3 and 4).

Written Assignment - Individual Assessment, 2 Credits. (Code: 0140)

The students have to hand in an individual assessment of another groups written assignment based on a number of provided criteria. (Assesses goals 3 and 4).

For further information, see the university's local examination regulations (in Swedish).

Grades

According to the Higher Education Ordinance, Chapter 6, Section 18, a grade is to be awarded on the completion of a course, unless otherwise prescribed by the university. The university may prescribe which grading system shall apply. The grade is to be determined by a teacher specifically appointed by the university (an examiner).

According to regulations on grading systems for first- and second-cycle education (vice-chancellor's decision 2010-10-19, reg. no. CF 12-540/2010), one of the following grades is to be used: fail, pass, or pass with distinction. The vice-chancellor or a person appointed by the vice-chancellor may decide on exceptions from this provision for a specific course, if there are special reasons.

Grades used on course are Fail (U), Pass (G) or Pass with Distinction (VG).

Analysis of Currently Reported Threats and Incidents

Grades used are Fail (U) or Pass (G).

Social Aspects

Grades used are Fail (U) or Pass (G).

Written Assignment - in Group

Grades used are Fail (U), Pass (G) or Pass with Distinction (VG).

Written Assignment - Individual Assessment

Grades used are Fail (U), Pass (G) or Pass with Distinction (VG).

FINAL GRADE

The final grade will be translated into the ECTS grading scale.

In order to receive the grade Pass, the student must be awarded Pass in all examination parts. In order to receive the grade Pass with Distinction, the student must be awarded Pass with Distinction in both Written Assignment and the grade Pass in all other examination parts.

For further information, see the university's local examination regulations (in Swedish).

Specific entry requirements

Informatics, Basic Course 30 Credits, 30 Credits at intermediate course level within Informatics and successful completion of at least 15 Credits at advanced course level within Informatics. Alternatively Business Administration, Basic Course, 30 Credits, Business Administration, Intermediate Course, 30 Credits and successful completion of at least 15 Credits at advanced course level within Business Administration. Alternatively 30 Credits within G1N in Computer Science and 45 Credits within G1F in Computer Science. The applicant must also have qualifications corresponding to the course "English 6" or "English B" from the Swedish Upper Secondary School.

For further information, see the university's admission regulations (in Swedish).

Transfer of Credits for Previous Studies

Students who have previously completed higher education or other activities are, in accordance with the Higher Education Ordinance, entitled to have these credited towards the current programme, providing that the previous studies or activities meet certain criteria.

For further information, see the university's local credit transfer regulations (in Swedish).

Other Provisions

Remaining tasks should be completed as soon as possible according to the teacher's instructions.

Reading List and Other Teaching Materials

Required Reading

Dhillon, Gurpreet (2018)
Information Security: Text & Cases
Prospect Press, 413 pages

Additions and Comments on the Reading List

Lärare kommer under kursen föreslå forskningsartiklar för de olika kursmodulerna. Uppskattningsvis 300 sidor./ Research papers related to the course modules will be suggested by the concerned teachers(s) during the course. Approximately 300 pages.