

## Studieplan 2013/2014

### Master in Information Security

#### Studieprogramkode

MIS

#### Innledning

Information technology permeates all aspects of society and has become critical to industry, government, and individual well-being. Securing the vital services and structures and ensuring availability of trustworthy information whenever and wherever it is required has become a field of intensive interdisciplinary research in the recent years. At the same time, information security has become an area of extensive commercial activity with thousands of companies developing and marketing various data protection products. The Master of science in information security provides the students with knowledge and theoretical background, as well as with the skills and attitudes necessary to succeed in this challenging yet eminently rewarding field.

The goals of the study program are achieved through the research-based courses that reflect the research results of the teaching staff to a large extent. This provides the students with thorough knowledge about modern information security technologies.

The study program is closely related to the research community Norwegian Information Security Laboratory (NISlab), which also offers bachelor and PhD studies in information security. This research environment consists of professors that are active in research and internationally recognized as experts in their respective fields. NISlab is a member of Forum for Research and Innovation in Security and Communication (FRISC), a Norwegian network of institutions dedicated to cutting-edge research in information security. NISlab also has strong international relations and its collaboration network includes more than 20 research institutions from more than 10 countries worldwide.

#### Studiets varighet, omfang og nivå

This is a two-year master program (120 ECTS credits), which is also available part-time over three or four years. The degree awarded upon completion is “Master in Information Security”.

The program has three tracks: **Technology**, **Digital forensics** and **Management**. After the first semester, which is common to all the tracks (see the course structure below), the students have to choose which track they are going to pursue.

The program qualifies the students to proceed to Ph.D. studies.

#### Forventet læringsutbytte

##### *Knowledge*

- The candidate possesses advanced knowledge in the field of information security in general and the following particular topics: computer and network security, security management, incident response, security of critical information infrastructure and legal aspects of information security. The candidate possesses special insight and expertise in information security technology, digital forensics or security management, depending on the chosen program track.
- The candidate possesses thorough knowledge of academic theory and methods in the field of

information security.

- The candidate is capable of applying knowledge in new areas within the field of information security.
- The candidate is familiar with current state-of-the-art in the field of information security.
- The candidate possesses thorough knowledge of scientific methodology, needed to plan and carry out research and development projects in the field of information security.

### *Skills*

- The candidate is capable of analyzing existing theories, methods and interpretations of theories within the field of information security as well as solving theoretical and practical problems independently.
- The candidate is capable of using independently relevant methods in research and development in the field of information security. These methods include literature study, logical reasoning and performing scientific experiments together with interpreting their results.
- The candidate is capable of performing critical analysis of different information sources and applying the results of that analysis in academic reasoning and structuring and formulating scientific problems.
- The candidate is capable of completing an independent research and development project of moderate size under supervision (example: the master thesis), adhering to the current code of ethics in scientific research.
- The candidate is capable of carrying out a plan of a research project under supervision.

### *General competence*

- The candidate is capable of analyzing academic, professional and research problems.
- The candidate is capable of using knowledge and skills to carry out advanced tasks and projects.
- The candidate is capable of imparting comprehensive independent work in the field of information security. The candidate also mastered the terminology in the field of information security.
- The candidate is capable of communicating academic issues, analysis and conclusions both with experts in the field of information security and with the general audience.
- The candidate is capable of contributing to innovation and innovation processes.

### **Målgruppe**

There are three focus groups for this study program:

1. Undergraduate students entering the program as a continuation of their bachelor degree without any prior work experience.
2. Industry students (or students in the private/public sector in general) looking for a full-time or part-time master program, which is flexible and can be adapted to their employers' needs and their own individual needs.
3. International students: exchange students (arriving for a single semester only), full-time students, and part-time students.

### **Opptakskrav og rangering**

To qualify for admission, an applicant must have a bachelor degree in computer science or another field relevant for information security (mathematics, electrical engineering, physics, etc.). The applicant must document that he/she has at least 10 ECTS credits in mathematics/statistics and at least 30 ECTS credits in computer science subjects (for example, computer programming, theory of

algorithms, databases, computer networking, etc.) at the bachelor level. A grade point average (GPA) of at least C on the bachelor studies is required.

Graduate studies in information security require a somewhat different mathematical platform than the one included in most bachelor studies. To master the theoretical topics included in the master program we recommend that the students attend the consultancy sessions related to certain topics in the field of mathematics, organized occasionally during the course of the studies.

### **Studiets innhold, oppbygging og sammensetning**

The program is offered in a flexible manner to fit well to all the three target groups of students. In general, on-campus presence is *required* only three times per semester (1-3 days each time), for a start-up session, for mid-term exams/presentations (and a start-up session of the second part of the semester) and for final exams/presentations. Attendance is also strongly recommended for the *initial first two weeks of the program when two preparatory intense short-courses in number theory and theoretical computer science are offered*. All courses are available online, but there will also be sessions on a regular weekly or bi-weekly schedule. The presence on these sessions is not required.

The program has three tracks (paths of study): technology, digital forensics, and management. Students have to choose which track they pursue after the first semester, which is common for all the tracks. The common courses in the first semester cover the core topics in both information security technology, forensics and management: Cryptology 1, Applied information security, IT governance, Legal aspects of information security, Digital forensics 1, and Scientific methodology. In the rest of the study program, each track has a set of specific courses. Elective courses, taken in the 3rd semester, are freely chosen from a common pool of electives. The students have to choose their master thesis topics within their chosen tracks.

Ordinary mandatory courses from other tracks of the program and courses from the master program in media technology and the CIMET (Color in Informatics and Media Technology) master may be included as electives. Students can also use *up to 20 ECTS of the courses at the 3000 level* as a part of their master program. These must however not be part of the necessary credits for admission – if so, they must be replaced by new credits. Some of the courses listed above can also be flexible regarding time, space and teaching format upon request by the students (typically, a course may be taken in a different semester through self-study and under individual or group supervision).

Master-level courses from other institutions may be included as electives or may substitute mandatory courses at the discretion of the program director.

The course structure for the part-time students may be composed individually as long the track-specific requirements mentioned above and any course inter-dependencies are respected. The most important course inter-dependencies are the following: 1. Students should start working on their master theses in the semester following the research project planning course, 2. All previous coursework has to be completed before starting work on the master thesis (an exception of 10 missing credits may be tolerated at the discretion of the director of the study program, but only if the missing credits are not relevant for the topic of the master thesis).

### **Study methods**

- Lectures
- Exercises
- Project work

- Essay/Article writing
- Independent study
- Group exercises
- Lab exercises

In addition to the classical study methods requiring presence by the students, the Master program in information security makes extensive use of flexible distance study methods. Every course contains the whole study material in digital form available online, via a special system available to the students once enrolled in the program. Audio recordings of the lectures are available online in most subjects contained in the program and the number of subjects that use video recording of the lectures is increasing very fast as technical possibilities make this form of presentations possible. Video streaming of the lectures is also used, whenever technical possibilities allow this. Many subjects use online exams and the exams requiring physical presence are often organized in distant places across Norway, depending on the number of interested participants.

### **Tekniske forutsetninger**

The students who choose to participate in the study program as distance students, need a broadband Internet connection. Software that is needed is mostly freely available on the Internet. In some courses, commercial products such as MatLab, are required.

As for the practical computer skills, it is expected that the students are capable of using any contemporary operating system (Microsoft Windows, GNU/Linux, MacOS, etc.) both with a graphical user interface and a command line interface.

### **Sensorordning**

Most courses have internal examiners, but some of them have external examiners. The subject Research project planning and the master thesis always have an external examiner.

### **Internasjonalisering**

The students are allowed to travel abroad to do their master theses. The information security group has strong links to many of the leading international academic groups within the field, and the students are encouraged to contact their instructors in the course «Research project planning» to ask for relevant travel opportunities.

### **Klar for publisering**

Ja

### **Utdanningsnivå**

Mastergrad

**Master in Information Security 2013-2015 Technology full-time track**

Emnekode	Emnets navn	O/V *)	Studiepoeng pr. semester			
			S1(H)	S2(V)	S3(H)	S4(V)
IMT4421	<u>Scientific methodology</u>	O	5			
IMT4532	<u>Cryptology 1</u>	O	5			
IMT4561	<u>Applied Information Security</u>	O	5			
IMT4571	<u>IT Governance</u>	O	5			
IMT4591	<u>Legal Aspects of Information Security</u>	O	5			
IMT4012	<u>Digital Forensics 1</u>	O	5			
IMT4152	<u>Socio-technical Security Risk Modeling and Analysis 1</u>	O			5	
IMT4582	<u>Network Security</u>	O			5	
IMT4541	<u>Foundations of Information Security</u>	O			5	
IMT4552	<u>Cryptology 2</u>	O			5	
IMT4621	<u>Biometrics</u>	O			5	
IMT4122	<u>Software Security Trends</u>	O			5	
	<u>Valgemne, 5 ECTS</u>	V				5
	<u>Valgemne, 5 ECTS</u>	V				5
	<u>Valgemne, 5 ECTS</u>	V				5
	<u>Valgemne, 5 ECTS</u>	V				5
	<u>Valgemne, 5 ECTS</u>	V				5
IMT4601	<u>Research Project Planning</u>	O				5
IMT4904	<u>Master Thesis</u>	O				30
Sum:			30	30	30	30

\*) O - Obligatorisk emne, V - Valgbare emne

**Master in Information Security 2013-2015 Digital Forensics full-time track**

Emnekode	Emnets navn	O/V *)	Studiepoeng pr. semester			
			S1(H)	S2(V)	S3(H)	S4(V)
IMT4421	<u>Scientific methodology</u>	O	5			
IMT4532	<u>Cryptology 1</u>	O	5			
IMT4561	<u>Applied Information Security</u>	O	5			
IMT4571	<u>IT Governance</u>	O	5			
IMT4591	<u>Legal Aspects of Information Security</u>	O	5			
IMT4012	<u>Digital Forensics 1</u>	O	5			
IMT4612	<u>Machine Learning and Pattern Recognition 1</u>	O			5	
IMT4582	<u>Network Security</u>	O			5	
IMT4641	<u>Computational Forensics</u>	O			5	
IMT4022	<u>Digital Forensics 2</u>	O			10	
IMT4122	<u>Software Security Trends</u>	O			5	
	<u>Valgemne, 5 ECTS</u>	V				5
	<u>Valgemne, 5 ECTS</u>	V				5
	<u>Valgemne, 5 ECTS</u>	V				5
	<u>Valgemne, 5 ECTS</u>	V				5
	<u>Valgemne, 5 ECTS</u>	V				5
IMT4601	<u>Research Project Planning</u>	O				5
IMT4904	<u>Master Thesis</u>	O				30
Sum:			30	30	30	30

\*) O - Obligatorisk emne, V - Valgbare emne

**Master in Information Security 2013-2015 Management full-time track**

Emnekode	Emnets navn	O/V *)	Studiepoeng pr. semester				
			S1(H)	S2(V)	S3(H)	S4(V)	
IMT4421	<u>Scientific methodology</u>	O	5				
IMT4532	<u>Cryptology 1</u>	O	5				
IMT4561	<u>Applied Information Security</u>	O	5				
IMT4571	<u>IT Governance</u>	O	5				
IMT4591	<u>Legal Aspects of Information Security</u>	O	5				
IMT4012	<u>Digital Forensics 1</u>	O	5				
IMT4152	<u>Socio-technical Security Risk Modeling and Analysis 1</u>	O			5		
IMT4582	<u>Network Security</u>	O			5		
IMT4651	<u>Security as Continuous Improvement</u>	O			5		
IMT4661	<u>Security Management Dynamics</u>	O			5		
IMT4841	<u>Security Planning and Incident Management</u>	O			10		
	<u>Valgemne, 5 ECTS</u>	V				5	
	<u>Valgemne, 5 ECTS</u>	V				5	
	<u>Valgemne, 5 ECTS</u>	V				5	
	<u>Valgemne, 5 ECTS</u>	V				5	
	<u>Valgemne, 5 ECTS</u>	V				5	
IMT4601	<u>Research Project Planning</u>	O				5	
IMT4904	<u>Master Thesis</u>	O					30
Sum:			30	30	30	30	

\*) O - Obligatorisk emne, V - Valgbare emne

**Master in Information Security 2013-2016 Technology part-time track (three years)**

Emnekode	Emnets navn	O/V *)	Studiepoeng pr. semester						
			S1(H)	S2(V)	S3(H)	S4(V)	S5(H)	S6(V)	
IMT4421	<u>Scientific methodology</u>	O	5						
IMT4532	<u>Cryptology 1</u>	O	5						
IMT4561	<u>Applied Information Security</u>	O	5						
IMT4012	<u>Digital Forensics 1</u>	O	5						
IMT4152	<u>Socio-technical Security Risk Modeling and Analysis 1</u>	O			5				
IMT4582	<u>Network Security</u>	O			5				
IMT4541	<u>Foundations of Information Security</u>	O			5				
IMT4552	<u>Cryptology 2</u>	O			5				
IMT4571	<u>IT Governance</u>	O				5			
IMT4591	<u>Legal Aspects of Information Security</u>	O				5			
	<u>Valgemne, 5 ECTS</u>	V				5			
	<u>Valgemne, 5 ECTS</u>	V				5			
IMT4122	<u>Software Security Trends</u>	O					5		
IMT4621	<u>Biometrics</u>	O					5		
	<u>Valgemne, 5 ECTS</u>	V					5		
	<u>Valgemne, 5 ECTS</u>	V					5		
IMT4601	<u>Research Project Planning</u>	O					5		
	<u>Valgemne, 5 ECTS</u>	V					5		
IMT4904	<u>Master Thesis</u>	O						10	20
Sum:			20	20	20	20	20	20	

\*) O - Obligatorisk emne, V - Valgbare emne

**Master in Information Security 2013-2016 Digital Forensics part-time track (three years)**

Emnekode	Emnets navn	O/V *)	Studiepoeng pr. semester					
			S1(H)	S2(V)	S3(H)	S4(V)	S5(H)	S6(V)
IMT4421	<u>Scientific methodology</u>	O	5					
IMT4532	<u>Cryptology 1</u>	O	5					
IMT4561	<u>Applied Information Security</u>	O	5					
IMT4012	<u>Digital Forensics 1</u>	O	5					
IMT4612	<u>Machine Learning and Pattern Recognition 1</u>	O		5				
IMT4582	<u>Network Security</u>	O		5				
IMT4641	<u>Computational Forensics</u>	O		5				
IMT4122	<u>Software Security Trends</u>	O		5				
IMT4571	<u>IT Governance</u>	O			5			
IMT4591	<u>Legal Aspects of Information Security</u>	O			5			
	<u>Valgemne, 5 ECTS</u>	V			5			
	<u>Valgemne, 5 ECTS</u>	V			5			
IMT4022	<u>Digital Forensics 2</u>	O				10		
	<u>Valgemne, 5 ECTS</u>	V				5		
	<u>Valgemne, 5 ECTS</u>	V				5		
IMT4601	<u>Research Project Planning</u>	O					5	
	<u>Valgemne, 5 ECTS</u>	V					5	
IMT4904	<u>Master Thesis</u>	O					10	20
		Sum:	20	20	20	20	20	20

\*) O - Obligatorisk emne, V - Valgbare emne

**Master in Information Security 2013-2016 Management part-time track (three years)**

Emnekode	Emnets navn	O/V *)	Studiepoeng pr. semester					
			S1(H)	S2(V)	S3(H)	S4(V)	S5(H)	S6(V)
IMT4421	<u>Scientific methodology</u>	O	5					
IMT4532	<u>Cryptology 1</u>	O	5					
IMT4561	<u>Applied Information Security</u>	O	5					
IMT4571	<u>IT Governance</u>	O	5					
IMT4152	<u>Socio-technical Security Risk Modeling and Analysis 1</u>	O		5				
IMT4582	<u>Network Security</u>	O		5				
IMT4651	<u>Security as Continuous Improvement</u>	O		5				
IMT4661	<u>Security Management Dynamics</u>	O		5				
IMT4012	<u>Digital Forensics 1</u>	O			5			
IMT4591	<u>Legal Aspects of Information Security</u>	O			5			
	<u>Valgemne, 5 ECTS</u>	V			5			
	<u>Valgemne, 5 ECTS</u>	V			5			
IMT4841	<u>Security Planning and Incident Management</u>	O				10		
	<u>Valgemne, 5 ECTS</u>	V				5		
	<u>Valgemne, 5 ECTS</u>	V				5		
IMT4601	<u>Research Project Planning</u>	O					5	
	<u>Valgemne, 5 ECTS</u>	V					5	
IMT4904	<u>Master Thesis</u>	O					10	20
		Sum:	20	20	20	20	20	20

\*) O - Obligatorisk emne, V - Valgbare emne

**Electives**

Emnekode	Emnets navn	O/V *)	Studiepoeng pr. semester	
			S1(H)	S2(V)
IMT3491	<u>Ethical Hacking and Penetration Testing</u>	V	5	
IMT3511	<u>Discrete Mathematics</u>	V		10
IMT3761	<u>Informasjonskrigføring</u>	V	5	
IMT4132	<u>IT Rhetorics for Security Risk Management</u>	V	5	
IMT4142	<u>Information Security Economics 1</u>	V	5	
IMT4671	<u>Organizational and Human Aspects of Information Security</u>	V	5	
IMT4722	<u>Behavioural Biometrics</u>	V	5	
IMT4741	<u>Intrusion detection and prevention</u>	V	5	
IMT4751	<u>Wireless communication security</u>	V	5	
IMT4762	<u>Risk Management 1</u>	V	5	
IMT4772	<u>Risk Management 2</u>	V	5	
IMT4881	<u>Specialization Course 1</u>	V	5	5
IMT4882	<u>Specialization Course 2</u>	V	10	10
Sum:			0	0

\*) O - Obligatorisk emne, V - Valgbare emne



## Emneoversikt

### IMT4421 Scientific methodology - 2013-2014

**Emnekode:**

IMT4421

**Emnenavn:**

Scientific methodology

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Varighet (fritekst):**

Første halvdel av semesteret

**Språk:**

Engelsk

**Forventet læringsutbytte:**

Etter endt emne skal studenten

**Kunnskap**

- kunne analysere sentrale problemstillinger innen vitenskapsteori
- ha inngående kunnskap om sentrale spørsmål innen vitenskapsteori
- kjenne sentral terminologi for vitenskapelige arbeider

**Ferdigheter**

- foreslå en vitenskapelig problemstilling
- selvstendig kunne planlegge gjennomføringen av et vitenskapelig arbeid
- kunne søke etter akademiske publikasjoner ved hjelp av sentrale databaser for dette
- kunne tilrettelegge og analysere data fra vitenskapelige prosjekter

**Generell kompetanse**

- kunne lese og analysere akademiske publikasjoner
- kunne rapportere resultater fra vitenskapelige prosjekter, deriblant egenutførte vitenskapelige arbeider
- ha utviklet bevisste etiske holdninger i forhold til hvordan vitenskapelig metodikk anvendes

**Emnets temaer:**

- Introduksjon til vitenskapsteori
- Hva kjennetegner god forskning
- Forskningsetikk
- Forskning som middel til systematisk fremgang
- Kvantitative og kvalitative forskningsdesign
- Hva karakteriserer gode problemstillinger og hvordan lager man en
- Litteraturstudier
- Metodevalg, inkludert planlegging, gjennomføring, og analyse av eksperimenter/studier.
- Bruk av forskningsdatabaser for problemløsning og forbedring
- Behandling av data/statistikk
- Utarbeidelse av prosjektplan
- Gjennomføring av risikoanalyse og gjennomførbarhetsanalyse

**Pedagogiske metoder:**

Essay  
Forelesninger  
Nettbasert Læring  
Prosjektarbeid  
Veiledning

**Pedagogiske metoder (fritekst):**

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (Fronter).

**Vurderingsformer:**

Skriftlig eksamen, 3 timer

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Intern og ekstern sensor.

**Utsatt eksamen (tidl. kontinuasjon):**

Ordinær kontinuasjoneksamen.

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Engelsk ordbok.

**Obligatoriske arbeidskrav:**

Godkjent essay

Gjennomført praktisk prosjekt

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Førstelektor Frode Volden

**Læremidler:**

Leedy, P D, and Ormrod, J E: "Practical Research, -Planning and design, 9th ed." Pearson Educational Int. ISBN-10: 0131365665

Samt tilleggslitteratur, utdelt eller gjort tilgjengelig i Fronter.

**Klar for publisering:**

Ja

**Emneside (URL):**

<http://www.hig.no/imt/mt/emnesider/imt4421>

## **IMT4532 Cryptology 1 - 2013-2014**

**Emnekode:**

IMT4532

**Emnenavn:**

Cryptology 1

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Varighet (fritekst):**

First half of the fall semester

**Språk:**

Engelsk

**Forventet læringsutbytte:****Knowledge**

- The candidate possesses advanced knowledge of classical cryptography, as well as of stream ciphers, block ciphers and public key ciphers.
- The candidate possesses thorough knowledge about theory and scientific methods relevant for cryptology.
- The candidate is capable of applying his/her knowledge in new fields of cryptology.

**Skills**

- The candidate is capable of analyzing existing theories, methods and interpretations in the field of cryptology and working independently on solving theoretical and practical problems.
- The candidate can use relevant scientific methods in independent research and development in cryptology.
- The candidate is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in cryptology.
- The candidate is capable of carrying out an independent limited research or development project in cryptology under supervision, following the applicable ethical rules.

**General competence**

- The candidate is capable of analyzing relevant professional and research ethical problems in cryptology.
- The candidate is capable of applying his/her cryptographic knowledge and skills in new fields, in order to accomplish advanced tasks and projects.
- The candidate can work independently and is familiar with cryptographic terminology.
- The candidate is capable of discussing professional problems, analyses and conclusions in the field of cryptology, both with specialists and with general audience.
- The candidate is capable of contributing to innovation and innovation processes.

**Emnets temaer:**

1. Classical cryptography - history of cryptography, fundamentals of information theory and its application in cryptography
2. Symmetric ciphers - stream and block ciphers
3. Asymmetric ciphers - fundamentals, RSA
4. Hash functions and digital signatures.

**Pedagogiske metoder:**

Forelesninger  
Oppgaveløsning  
Prosjektarbeid

**Pedagogiske metoder (fritekst):**

Lectures

Numerical exercises

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

Project work

**Vurderingsformer:**

Skriftlig eksamen, 3 timer

Vurdering av prosjekt(er)

**Vurderingsformer:**

Written exam, 3 hours, counts for 70% of the final mark

Project, counts for 30% of the final mark

Both exam and project must be passed

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Evaluated by the lecturer. An external examiner will be used every 4th year. Next time in the school-year 2014/2015.

**Utsatt eksamen (tidl. kontinuasjon):**

Ordinary re-sit examination. The project work (if passed) need not be repeated.

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Calculator, dictionary

**Obligatoriske arbeidskrav:**

None

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Professor Slobodan Petrovic

**Læremidler:****Books:**

1. Introduction to Cryptography and Coding Theory, 2. edition, Trappe W., Washington L., Prentice Hall, 2006, ISBN: 0131981994.

2. Handbook of Applied Cryptography, Menezes A., <http://www.cacr.math.uwaterloo.ca/hac>

**Erstatter:**

IMT4531 Introduction to Cryptology

**Supplerende opplysninger:**

There is room for 50 students on the course.

The students that has already taken course IMT3771 Introduction to cryptology at the bachelor level and continues with the master's program in information security at HiG cannot be exempted from taking the course IMT4532 Cryptology 1 on the master's level since the expected learning outcomes and the evaluation methods in these two courses are different (the written exam is different and there is a compulsory project in IMT4532).

**Klar for publisering:**

Ja

**Emneside (URL):**

<http://www.hig.no/imt/emnesider/imt4532>

## IMT4561 Applied Information Security - 2013-2014

**Emnekode:**

IMT4561

**Emnenavn:**

Applied Information Security

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Språk:**

Engelsk

**Forventet læringsutbytte:****Knowledge**

- Candidates should have a solid grounding in core concepts of information security and privacy
- Candidates possess advanced knowledge of security design principles and their influence on security policies and security architecture
- Candidates have advanced knowledge of common vulnerabilities, attack mechanisms, and methods against computer and information systems
- Candidates have thorough knowledge on the theory and methods underlying access control as well as of identification and authentication mechanisms

**Skills**

- Candidates are capable of applying relevant methods for independent analysis and research on security architectures, their vulnerabilities, and potential attacks against these
- Candidates are able to analyze and critically review literature in the field of information security and are able to apply results from the literature in structuring and formulating arguments and reasoning on information security topics
- Candidates are able to plan and conduct a limited, guided research exercise based on primary literature resulting in a reasoned and coherent report

**General Competence**

- Candidates are able to conduct translate knowledge and methods in the area of information security to onvel fields so as to be able to successfully complete advanced tasks and projects in information security
- Candidates are able to work independently and are familiar with core concepts and problems in information security and security architecture
- Candidates are able to contribute to innovations and innovative processes, identifying advanced information security problems and approaches contributing to their solution



**Emnets temaer:**

- Core concepts in information security and privacy
- Security design principles
- Security policies
- Security architecture: Operating systems and applications
- Access control principles
- Identification and authentication
- Vulnerabilities and attack mechanisms
- Attack methods and malicious software
- Database security

**Pedagogiske metoder:**

Forelesninger

Annet

**Pedagogiske metoder (fritekst):**

- Lectures
- Other (tutorials)
- Other (term paper)

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Annet

**Vurderingsformer:**

Assessment consists of two parts, pass decision is on cumulative grade of both parts:

- Part 1 is a written examination (3 hours), accounting for 67% of grade
- Part 2 is a term paper, accounting for 33% of grade.

Term paper is evaluated by the lecturer.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Evaluated by external and internal examiner.

**Utsatt eksamen (tidl. kontinuasjon):**

A new term paper must be provided and the examination must be re-sat next autumn.

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Dictionary, simple calculator

**Obligatoriske arbeidskrav:**

None.

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Professor Stephen Wolthusen

**Læremidler:**

The following textbooks are the primary references; further recommended reading is provided in the course syllabus.

D. Gollmann: Computer Security, 3rd edition Wiley, 2011

M. Bishop: Computer Security: Art and Science. Addison-Wesley, 2003.

R. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems (2nd edition). John Wiley & Sons, Chichester, UK (2008)

**Erstatter:**

IMT4162 Information Security and Security Architecture

**Klar for publisering:**

Ja

## IMT4571 IT Governance - 2013-2014

**Emnekode:**

IMT4571

**Emnenavn:**

IT Governance

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Varighet (fritekst):**

Andre halvdel av semesteret

**Språk:**

Engelsk

## Forventet læringsutbytte:

### Knowledge

- The candidate possesses detailed knowledge of IT Governance principles and procedures, and the basic concepts of the ISO 27001 / ISO 27002 standard.
- The candidate possesses thorough knowledge about the overall process for establishment and maintenance of an Information Security Management Systems (ISMS).
- The candidate possesses detailed knowledge about the role of policies, standards and guidelines for controls and is capable of applying his/her knowledge in case studies.

### Skills

- The candidate is capable of applying IT Governance principles on practical case-studies, including proposal and evaluation of technical security architectures and solutions.
- The candidate is capable of performing stakeholder analysis, risk assessment and recommending risk treatment plans on limited case-studies.
- The candidate is capable of evaluating the applicability of common security mechanism for various controls given a certain scope and policy for the control.

### General competence

- The candidate is capable of analyzing business and organizational needs for an ISMS and has a thorough understanding of security management as a continuous improvement process.
- The candidate can work independently and is familiar with IT Governance terminology.
- The candidate is capable of discussing professional problems such as documentation, decision making processes, implementation plans, operations, reviews and corrective actions, with both IT specialists and general managers.

**Emnets temaer:**

- Reasons for IT Governance: Compliance, liability, stability
- Organizing information security
- Information security policy and scope
- The risk assessment and statement of applicability
- Identification of risks related to external parties
- Asset management
- Human resources security
- Physical and environmental security
- Equipment security
- Communications and operations management
- Controls against malicious software (malware) and back-ups
- Network security management and media handling
- Exchanges of information
- Electronic commerce services
- E-mail and internet use
- Access control
- Network access control
- Operating system access control
- Application access control and teleworking
- Systems acquisition, development and maintenance
- Cryptographic controls
- Security in development and support processes
- Monitoring and information security incident management
- Business continuity management
- Compliance
- Principles of auditing

**Pedagogiske metoder:**

Annet

**Pedagogiske metoder (fritekst):**

Lectures, exercises and projects.

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Annet

**Vurderingsformer:**

- 1-2 Multiple Choice Tests (weight: 20%)
- 1-2 group Assignments (weight: 30%)
- Digital Final exam, 2 hours (weight: 50%)

The final digital exam is conducted in Fronter with students present in the computer lab at HiG  
All three parts are mandatory and must be passed!

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Evaluated by the lecturer. An external examiner will be used every 4th year. Next time in the school-year 2014/2015.

**Utsatt eksamen (tidl. kontinuasjon):**

For the final exam: Ordinary re-sit examination.

**Tillatte hjelpemidler:****Obligatoriske arbeidskrav:**

None.

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Forskningsjef Åsmund Skomedal

**Læremidler:**

Literature:

Alan Calder & Steve Watkins. IT Governance : IT Governance: A Manager's Guide to Data Security and ISO 27001 / ISO 27002. Fifth Edition. Kogan Page. 2008.

Anderson, Ross (1999) Why cryptosystems fail, University Computer Laboratory, University of Cambridge, Cambridge, UK, <http://www.cl.cam.ac.uk/~rja14/wcf.html>.

**Klar for publisering:**

Ja

## IMT4591 Legal Aspects of Information Security - 2013-2014

**Emnekode:**

IMT4591

**Emnenavn:**

Legal Aspects of Information Security

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Språk:**

Norsk, alternativt engelsk

**Forventet læringsutbytte:*****Knowledge***

- The candidate possesses advanced knowledge in legal aspects especially relevant for information security. This applies particularly to the legal regulation of matters of importance to safeguarding confidentiality, integrity, access and quality.

***Skills***

- The candidate is capable of performing critical analysis of various literature sources regarding legal aspects of information security.
- The candidate is capable of carrying out an independent limited research or development project in legal aspects of information security under supervision, following the applicable ethical rules.

***General competence***

- The candidate is capable of analyzing relevant professional and research ethical problems in legal aspects of information security.
- The candidate is capable of applying his/her knowledge about legal aspects of information security in new fields, in order to accomplish advanced tasks and projects.
- The candidate can work independently and is familiar with legal terminology.

**Emnets temaer:**

Generelle bestemmelser om informasjonssikkerhet, særlig innenfor e-forvaltning

Sikring av personopplysninger ved innsamling, bearbeiding og lagring av opplysninger

Regler for elektronisk kommunikasjon

**Pedagogiske metoder:**

Forelesninger  
Gruppearbeid  
Oppgaveløsning  
Samling(er)/seminar(er)

**Pedagogiske metoder (fritekst):**

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Skriftlig eksamen, 3 timer

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Intern + ekstern sensor

**Utsatt eksamen (tidl. kontinuasjon):**

Ingen ordinær kontinuasjon

**Tillatte hjelpemidler:****Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Timelærer Lise Nilsen

**Læremidler:**

Se oversikt i emnets rom i Fronter.

**Klar for publisering:**

Ja



## IMT4012 Digital Forensics 1 - 2013-2014

**Emnekode:**

IMT4012

**Emnenavn:**

Digital Forensics 1

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Språk:**

Engelsk

**Forutsetter bestått:**

se engelsk versjon

**Anbefalt forkunnskap:**

se engelsk versjon

**Forventet læringsutbytte:**

se engelsk versjon

**Emnets temaer:**

se engelsk versjon

**Pedagogiske metoder:**

Forelesninger

Lab.øvelser

Prosjektarbeid

**Vurderingsformer:**

Muntlig fremføring

Skriftlig eksamen, 3 timer

Vurdering av prosjekt(er)

**Vurderingsformer:**

se engelsk versjon

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

se engelsk versjon

**Utsatt eksamen (tidl. kontinuasjon):**

se engelsk versjon

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

se engelsk versjon

**Obligatoriske arbeidskrav:**

se engelsk versjon

**Ansvarlig avdeling:**

Avdeling for teknologi, økonomi og ledelse

**Emneansvarlig:**

Associate Professor André Årnes (andre.arnes@hig.no)

**Læremidler:**

se engelsk versjon

**Supplerende opplysninger:**

se engelsk versjon

**Klar for publisering:**

Ja

## **IMT4152 Socio-technical Security Risk Modeling and Analysis 1 - 2013-2014**

**Emnekode:**

IMT4152

**Emnenavn:**

Socio-technical Security Risk Modeling and Analysis 1

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Vår

**Varighet (fritekst):**

Andre halvdel av semesteret.

**Språk:**

Engelsk

**Forventet læringsutbytte:**

Se engelsk versjon.

**Emnets temaer:**

Se engelsk versjon.

**Pedagogiske metoder:**

Forelesninger

**Vurderingsformer:**

Essay

Skriftlig eksamen, 2 timer

**Vurderingsformer:**

Se engelsk versjon.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Tillatte hjelpemidler:**

**Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Ingen

**Obligatoriske arbeidskrav:**

Ingen

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Professor Stewart Kowalski

**Læremidler:**

Systems Thinking. System Dynamics: Managing Change and Complex . Kambiz. E. Maani, Robert Y. Cavana ,2 Ed Pearsons 2007.

Roadmap to Information Security, For IT and Infosec Managers, Michael E Whitman, Hervert J Mattord,, Course Technology 2011.

Related articles

Compendium.

**Erstatter:**

IMT4481

**Klar for publisering:**

Ja

## IMT4582 Network Security - 2013-2014

**Emnekode:**

IMT4582

**Emnenavn:**

Network Security

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Vår

**Varighet (fritekst):**

Se engelsk versjon.

**Språk:**

Engelsk

**Anbefalt forkunnskap:**

Se engelsk versjon

**Forventet læringsutbytte:**

Se engelsk versjon

**Emnets temaer:**

Se engelsk versjon

**Pedagogiske metoder:**

Essay

Forelesninger

**Vurderingsformer:**

Annet

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Se engelsk versjon

**Utsatt eksamen (tidl. kontinuasjon):**

Se engelsk versjon

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Ingen

**Obligatoriske arbeidskrav:**

Ingen

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Adjunct Professor Bernhard Hämmerli

**Læremidler:**

Se engelsk versjon.

**Erstatter:**

IMT4101 Sikkerhet i distribuerte systemer

**Klar for publisering:**

Ja

## **IMT4651 Security as Continuous Improvement - 2013-2014**

**Emnekode:**

IMT4651

**Emnenavn:**

Security as Continuous Improvement

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Vår

**Varighet (fritekst):**

Andre halvdel av vår semesteret

**Språk:**

Engelsk

**Forutsetter bestått:**

IMT4661 - Security Management Dynamics

**Forventet læringsutbytte:****Knowledge**

- The candidate possesses thorough knowledge of the fundamentals of security management for continuous improvement, as well as the factors that influence the behavior of security systems with regards to continuous improvement.
- The candidate possesses advanced knowledge about theory and scientific methods relevant modeling the dynamics of systems, in particular of security systems.

**Skills**

- The candidate is capable of analyzing existing theories, methods and interpretations in the field of security management and working independently on solving theoretical and practical problems of continuous improvement of security.
- The candidate can use relevant scientific methods in research and development in security management problems with regards to continuous improvement.
- The candidate is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in security management problems with regards to continuous improvement.
- The candidate is capable of carrying out an independent limited research or development project in security management problems with regards to continuous improvement under supervision, following the applicable ethical rules.
- The candidate is capable of applying his/her knowledge in problems of in security management with regards to continuous improvement.

**General competence**

- The candidate is capable of analyzing relevant professional and research ethical problems in security management with regards to continuous improvement.
- The candidate is capable of applying his/her security management knowledge and skills in new fields, in order to accomplish advanced tasks and projects.
- The candidate can work independently and is familiar with security management terminology.
- The candidate is capable of discussing professional problems, analyses and conclusions in the field of security management, both with specialists and with general audience.
- The candidate is capable of contributing to innovation and innovation processes.

**Emnets temaer:**

- The quality improvement paradox
- Security and quality improvement processes
- Improving the Performance of Computer Security Incident Response Teams (CSIRTs)
- Incident reporting systems and Learning from incidents
- Security risks in the transition to Integrated Operations
- Security-dependent safety. Continuous improvement of security in Critical Infrastructure

**Pedagogiske metoder:**

Forelesninger  
Oppgaveløsning  
Prosjektarbeid



**Pedagogiske metoder (fritekst):**

Web-enabled course with forum

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Flervalgstest(er)

Vurdering av prosjekt(er)

**Vurderingsformer:**

- Two multiple choice exams counting each 15%
- Two individual projects (papers) counting each 35%
- Each part must be individually approved of

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Evaluated by the lecturer. An external examiner will be used every 4th year. Next time in the school-year 2014/2015.

**Utsatt eksamen (tidl. kontinuasjon):**

The whole course must be repeated

**Tillatte hjelpemidler:****Obligatoriske arbeidskrav:**

The course requires active participation in projects – both in class and outside class.

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Professor Jose Gonzalez

**Læremidler:**

Written material will be given/sent to the students during the semester.

**Supplerende opplysninger:**

Hands-on modelling exercises during class are best carried out in computer lab. Students are encouraged to bring laptops to the classroom.

**Klar for publisering:**

Ja

## **IMT4661 Security Management Dynamics - 2013-2014**

**Emnekode:**

IMT4661

**Emnenavn:**

Security Management Dynamics

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Vår

**Varighet (fritekst):**

Første halvdel av vår semesteret

**Språk:**

Engelsk

**Forventet læringsutbytte:****Knowledge**

- The candidate possesses thorough knowledge of the fundamentals of security management, as well as the factors that influence the behavior of security systems with regards to MTO (“man-technology-organization”).
- The candidate possesses basic knowledge about theory and scientific methods relevant modeling the dynamics of systems, in particular of security systems.

**Skills**

- The candidate is capable of analyzing existing theories, methods and interpretations in the field of security management and working independently on solving theoretical and practical problems of moderate complexity.
- The candidate can use relevant scientific methods in research and development in security management problems of moderate complexity.
- The candidate is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in security management problems of moderate complexity.
- The candidate is capable of carrying out an independent limited research or development project in security management problems of moderate complexity under supervision, following the applicable ethical rules.
- The candidate is capable of applying his/her knowledge in problems of moderate complexity in security management.

**General competence**

- The candidate is capable of analyzing relevant professional and research ethical problems in security management.
- The candidate is capable of applying his/her security management knowledge and skills in new fields, in order to accomplish advanced tasks and projects.
- The candidate can work independently and is familiar with security management terminology.
- The candidate is capable of discussing professional problems, analyses and conclusions in the field of security management, both with specialists and with general audience.
- The candidate is capable of contributing to innovation and innovation processes.

**Emnets temaer:**

- Foundations – Security standards from the perspective of change and dynamics
- Introduction to qualitative system dynamics: Causal loop diagrams; System archetypes
- Modelling security management dynamics using system archetypes and causal loop diagrams
- Introduction to quantitative system dynamics: Causal structure and dynamic behaviour. Introduction to stocks and flows. Time delays.
- Basic system dynamics models of security management.

**Pedagogiske metoder:**

Forelesninger

Oppgaveløsning

Prosjektarbeid

**Pedagogiske metoder (fritekst):**

Web-enabled course with forum

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Flervalgstest(er)

Vurdering av prosjekt(er)

**Vurderingsformer:**

- Two multiple choice exams counting each 15%
- Two individual projects (papers) counting each 35%
- Each part must be individually approved of

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Evaluated by the lecturer. An external examiner will be used every 4th year. Next time in the school-year 2014/2015.

**Utsatt eksamen (tidl. kontinuasjon):**

The whole course must be repeated.

**Tillatte hjelpemidler:****Obligatoriske arbeidskrav:**

The course requires active participation in projects – both in class and outside class.

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Professor Jose Gonzalez

**Læremidler:**

Literature:

Maani, Kambiz E.; Cavana, Robert Y. Systems Thinking And Modelling. Pearson Education. 9781877371035.

Lectures, exercises and projects by Jose J. Gonzalez in Classfronter

**Erstatter:**

IMT4111 Sikkerhetsledelse

**Supplerende opplysninger:**

Hands-on modelling exercises during class are best carried out in computer lab. Students are encouraged to bring laptops to the classroom.

**Klar for publisering:**

Ja

## **IMT4841 Security Planning and Incident Management - 2013-2014**

**Emnekode:**

IMT4841

**Emnenavn:**

Security Planning and Incident Management

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

10

**Varighet:**

Vår

**Varighet (fritekst):**

Ett semester

**Språk:**

Norsk, alternativt engelsk

**Forventet læringsutbytte:****Kunnskap**

Studenten har etter fullført emne generell kunnskap om sikkerhetsplanlegging og hendelseshåndtering samt fordypning i ett av emnets temaer gjennom det selvstendige prosjektarbeidet.

Den generelle kunnskapen omfatter beredskapsplanlegging for håndtering av forretningskritiske hendelser. Det blir lagt vekt på både mindre hendelser og større hendelser hvor det kan være nødvendig å flytte drift til en annen lokasjon.

**Ferdigheter**

Studenten er i stand til å utarbeide beredskapsplaner for større og mindre informasjonssikkerhetshendelser.

Studenten er i stand til å lede planleggingsprosessen på en selvstendig måte.

**Generell kompetanse**

Studenten er i stand til selvstendig å fremskaffe informasjon/litteratur som omhandler sikkerhetsplanlegging og hendelseshåndtering. Videre er studenten i stand til å kritisk vurdere denne informasjonen og bruke den aktivt i beredskapsplanleggingsprosessen.

Studenten er i stand til å kommunisere overnevnte informasjon til andre.

**Emnets temaer:**

1. Introduksjon og overblikk over hendelseshåndtering beredskapsplanlegging.
2. Planlegging for en beredkapsorganisasjon: Risikostyring, risikostyringens begrensninger, hendelsesrapporteringssystemer, konsekvensanalyse
3. Hendelseshåndtering: forberedelse, organisering, preventive tiltak, deteksjon, hendelsesmelding, reaksjon, gjenoppbygging, vedlikehold, operasjonelle problemer for CSIRTs, og organisasjonsmodeller for CSIRTs.
4. Katastrofeshåndtering: Forberedelse, gjennomføring, drift og vedlikehold.
5. Kontinuitetsplanlegging: Forberedelse, gjennomføring, drift og vedlikehold.
6. Krisehåndtering og menneskelige faktorer.

**Pedagogiske metoder:**

Essay  
Forelesninger  
Nettbasert Læring  
Nettstøttet læring  
Refleksjon  
Veiledning

**Pedagogiske metoder (fritekst):**

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Skriftlig eksamen, 3 timer  
Vurdering av prosjekt(er)

**Vurderingsformer:**

Totalvurdering bestående av 100 poeng hvorav 50 poeng kan oppnåes på prosjektarbeide og 50 poeng på avsluttende 3-timers eksamen. Omregning fra 100-poengskala til A-F-skala skjer i henhold til anbefalt omregningstabell, men emneansvarlig kan i spesielle tilfeller gjøre små justeringer av grenser for å sikre overenstemmelse med de kvalitative beskrivelsene på A-F-skalaen. Både eksamen og prosjektarbeidet må bestås.

Prosjektarbeidet består av et selvstendig arbeid hvor studenten selv må fordype seg i et av emnets temaer. Studenten vil bli veiledet og motta tilbakemeldinger på arbeidet underveis.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Internal examiner. An external examiner will be used every 4th year. Next time in the school-year 2014/2015.

**Utsatt eksamen (tidl. kontinuasjon):**

Ordinær kontinuasjon på skriftlig eksamen

**Tillatte hjelpemidler:**

**Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Ordbok: Engelsk-Norsk, Norsk til annet språk eller Engelsk til annet språk.

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Associate professor Marie Gaup Moe

**Læremidler:**

Michael Whitman og Herbert Mattord: Principles of Incident Response and Disaster Recovery. Thomson, 2007.

Tilleggs litteratur vil bli utdelt eller gjort tilgjengelig på Fronter.

**Erstatter:**

IMT5161 - Incident response and computer forensics

**Supplerende opplysninger:**

Dette emnet er tilpasset studenter som følger fleksible-master-programmet og som ikke er tilstede på campus. Alle forelesninger kringkastes over internett i sanntid og lagres også slik at de kan ses i etterkant. Det tas opp både bilde og lyd. Veiledningsmøter kan gjennomføres online så lenge studenten har mikrofon tilgjengelig. Et webcam anbefales også.

Emnet undervises parallelt med bacheloremnet IMT3521.

Students that have already taken course IMT3521 Introduction to security Planning and Incident Handling at bachelor level cannot apply to be exempted from taking IMT4841 Security Planning and Incident Management when studying Master in Information Security, because expected learning outcomes in both courses are different.

**Klar for publisering:**

Ja



## Valgemne, 5 ECTS - 2013-2014

**Emnenavn:**

Valgemne, 5 ECTS

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Språk:**

Engelsk

**Forventet læringsutbytte:**

Knowledge

Skills

General competence

**Emnets temaer:**

1.

2.

...

**Pedagogiske metoder:**

Forelesninger

**Vurderingsformer:**

Skriftlig eksamen, 3 timer

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Tillatte hjelpemidler:****Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Prof. Slobodan Petrovic

**Klar for publisering:**

Ja

## IMT4601 Research Project Planning - 2014-2015

**Emnekode:**

IMT4601

**Emnenavn:**

Research Project Planning

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

Vår

**Varighet (fritekst):**

See English version

**Språk:**

Engelsk

**Forutsetter bestått:**

IMT4421 Scientific Methodology or

IMT4192 Research and Scientific Methods in HCI

**Forventet læringsutbytte:**

See English version

**Emnets temaer:**

See English version

**Pedagogiske metoder:**

Forelesninger

**Pedagogiske metoder (fritekst):**

See English version

**Vurderingsformer:**

Vurdering av prosjekt(er)

**Vurderingsformer:**

See English version

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

See English version

**Utsatt eksamen (tidl. kontinuasjon):**

See English version

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

See English version

**Obligatoriske arbeidskrav:**

See English version

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Einar Snekkenes](#)

**Emneansvarlig:**

Professor Einar Snekkenes

**Læremidler:**

See English version

**Supplerende opplysninger:**

See English version

**Klar for publisering:**

Ja

**Emneside (URL):**

<http://www.hig.no/imt/emnesider/imt4601>

## IMT4904 Master Thesis - 2014-2015

**Emnekode:**

IMT4904

**Emnenavn:**

Master Thesis

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

30

**Varighet:**

Høst

Vår

**Varighet (fritekst):**

Se engelsk beskrivelse.

**Gjelder fra vårsemesteret 2013.****Språk:**

Norsk, alternativt engelsk

**Forutsetter bestått:**

Se engelsk beskrivelse.

**Forventet læringsutbytte:**

Se engelsk beskrivelse.

**Emnets temaer:**

Se engelsk beskrivelse.

**Pedagogiske metoder:**

Prosjektarbeid

Samling(er)/seminar(er)

Veiledning

**Vurderingsformer:**

Annet

**Vurderingsformer:**

Se engelsk beskrivelse.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Se engelsk beskrivelse.

**Utsatt eksamen (tidl. kontinuasjon):**

Se engelsk beskrivelse.

**Tillatte hjelpemidler:****Obligatoriske arbeidskrav:**

Se engelsk beskrivelse.

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Vicedean/Dean

**Supplerende opplysninger:**

Se engelsk emnebeskrivelse

**Klar for publisering:**

Ja

**Emneside (URL):**

<http://www.hig.no/imt/emnesider/imt4901>

## IMT3491 Ethical Hacking and Penetration Testing - 2015-2016

**Emnekode:**

IMT3491

**Emnenavn:**

Ethical Hacking and Penetration Testing

**Faglig nivå:**

Bachelor (syklus 1)

**Studiepoeng:**

5

**Varighet:**

Høst

**Språk:**

Engelsk

**Forutsetter bestått:**

IMT2282 Operating systems

**Anbefalt forkunnskap:**

Master students must document that they have achieved learning outcomes equivalent to IMT2282 Operating systems

**Forventet læringsutbytte:**

Knowledge:

- Explain how a penetration test is planned, executed, documented and terminated.
- Account for vulnerabilities in general and common services running on internal and external servers for a generic company.
- Predict client side vulnerabilities and use the new methods for security breaches that may occur here.

Skills:

- Master the most common hacking and penetration testing tools and apply these tools to perform simple penetration testing tasks.
- Carry out structured and effective search for security issues in computer systems and computer networks.
- Construct effective penetration tests given existing threats towards software, networks, and network services.
- Use and abuse access to one system in order to gather more information about the networks and services used by this system.

General competence:

- Awareness of vulnerabilities in software both at server and client side, with an extra focus on network applications.
- Sensitivity for potential vulnerabilities in the computer systems and networks of a generic company, and ability to make an analysis of potential threats based on a network description.
- Overview of a wide set of tools for testing and accessing systems and networks.

**Emnets temaer:**

- Ethical hacking and penetration testing – definitions
- Penetration testing methodologies
- Hands-on penetration testing

**Pedagogiske metoder:**

Forelesninger

Gruppearbeid

Lab.øvelser

Oppgaveløsning

**Pedagogiske metoder (fritekst):**

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (Fronter).

**Vurderingsformer:**

Skriftlig eksamen, 2 timer

Vurdering av prosjekt(er)

Digital eksamen (leveringsform se tekstfelt)

**Vurderingsformer:**

- Digital OR written exam, (66%), depending on the number of students the exam might be oral
- Project (34%)
- Both parts must be passed

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Evaluated by internal examiner. External examiner is used periodically (every four years, next time in 2014/2015).

**Utsatt eksamen (tidl. kontinuasjon):**

- No re-sit examination – projects and exam are closely connected and related
- New project(s) and exam at next course dates

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

None.

**Obligatoriske arbeidskrav:**

One or two approved exercises, further information announced at course start.

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Basel Katt](#)

**Emneansvarlig:**

Basel Katt

**Læremidler:**

Engebretson, P. (2013). The Basics of Hacking and Penetration Testing 2nd Ed.

Supporting literature

Regalado, D., Harris, S., Harper, A., Eagle, C., Ness, J., Spasojevic, B., Linn, R., Sims, S. (2015): Gray Hat Hacking The Ethical Hacker's Handbook 4th Ed.

**Supplerende opplysninger:**

In case there will be less than 5 students that will apply for the course, it will be at the discretion of Studieprogramansvarlig whether the course will be offered or not and if yes, in which form.

There will also be an upper limit to the class based on available laboratory resources.

**Klar for publisering:**

Ja



## IMT3511 Discrete Mathematics - 2015-2016

**Emnekode:**

IMT3511

**Emnenavn:**

Discrete Mathematics

**Faglig nivå:**

Bachelor (syklus 1)

**Studiepoeng:**

10

**Varighet:**

Vår og høst

**Språk:**

Engelsk

**Forventet læringsutbytte:**

Se engelsk versjon.

**Emnets temaer:**

Se engelsk versjon.

**Pedagogiske metoder:**

Forelesninger

Oppgaveløsning

Veiledning

**Vurderingsformer:**

Muntlig, individuelt

**Vurderingsformer:**

Se engelsk versjon

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Se engelsk versjon

**Utsatt eksamen (tidl. kontinuasjon):**

Se engelsk versjon

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Se engelsk versjon

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Patrick Bours](#)

**Emneansvarlig:**

Professor Patrick Bours

**Læremidler:**

- Kenneth H. Rosen: Discrete Mathematics and its Applications, 7th edition, McGraw-Hill International Edition (2012), ISBN 978-0-07-338309-5
- William J. Gilbert and W. Keith Nicholson: Modern Algebra with Applications, 2nd edition, Wiley (2004), ISBN 0-471-41451-4

**Supplerende opplysninger:**

In case there will be less than 5 students that will apply for the course, it will be at the discretion of Studieprogramansvarlig whether the course will be offered or not and if yes, in which form.

**Klar for publisering:**

Ja

## IMT3761 Informasjonskrigføring - 2015-2016

**Emnekode:**

IMT3761

**Emnenavn:**

Informasjonskrigføring

**Faglig nivå:**

Bachelor (syklus 1)

**Studiepoeng:**

5

**Varighet:**

Høst

**Varighet (fritekst):**

Siste halvdel av høstsemester

**Språk:**

Norsk

**Forventet læringsutbytte:*****Kunnskap***

- Forklare hva informasjonskrigføring er
- Formulere hvordan informasjonskrigføring benyttes i krigføring, terrorisme og kriminalitet
- Gjøre rede for hvordan næringsliv og offentlig sektor kan beskytte seg mot informasjonskrigføring

***Ferdigheter***

- Følge reelle informasjonsoperasjoner
- Avsløre og gjenkjenne forsøk på psykologisk manipulasjon
- Velge indikatorer for å påvise at man er utsatt for informasjonskrigføring
- Planlegge og tilrettelegge for beskyttelse av bedrifter eller organisasjoner mot informasjonskrigføring

***Generell kompetanse***

- Anerkjenne samfunnets avhengighet av informasjonssystemer og at denne avhengigheten gjennom psykologisk manipulering, etterretning og målrettet ødeleggelse kan brukes til å utøve makt overfor enkeltpersoner, grupper og nasjonalstater
- Ta ansvar for beskyttelse av bedrifter eller organisasjoner i tråd med juridiske føringer

**Emnets temaer:**

- Informasjonskrigføringens terminologi og innhold
- Cyber space som operasjonsmiljø
- Våpen som brukes i informasjonskrigføring
- Introduksjon til psykologien bak manipulering
- Kunnskapsledelse (knowledge management)
- Verdivurdering
- Kunnskapsbaserte cyber-operasjoner

**Pedagogiske metoder:**

Forelesninger  
Gruppearbeid

**Pedagogiske metoder (fritekst):**

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (Fronter).

**Vurderingsformer:**

Skriftlig eksamen, 3 timer

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Sensureres av intern sensor, ekstern sensor benyttes periodisk (hvert fjerde år, neste gang i studieåret 2016/2017)

**Utsatt eksamen (tidl. kontinuasjon):**

Kontinuasjon/utsatt eksamen august 2016.

**Tillatte hjelpemidler:****Obligatoriske arbeidskrav:**

Rapporter

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Roger Johnsen](#)

**Emneansvarlig:**

Roger Johnsen

**Læremidler:**

Bøker:

- Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages, Andy Jones / Gerald L. Kovacich / Perry G. Luzwick, Auerbach Pub, utgave 1 (ISBN: 0849311144)
- Påvirkning. Teori og praksis., Robert B. Cialdini, utgave 2003 (ISBN: 82-7935-107-8)

**Supplerende opplysninger:**

Emnet har plass til max. 30 studenter.

Ingen opptak av forelesninger, frammøte anbefales.

**Klar for publisering:**

Ja

## **IMT4132 IT Rhetorics for Security Risk Management - 2015-2016**

**Emnekode:**

IMT4132

**Emnenavn:**

IT Rhetorics for Security Risk Management

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Varighet (fritekst):**

Second half of the autumn semester.

**Språk:**

Engelsk

**Forventet læringsutbytte:**

Se engelsk versjon.

**Emnets temaer:**

Se engelsk versjon.

**Pedagogiske metoder:**

Forelesninger

Lab.øvelser

**Vurderingsformer:**

Essay

Muntlig, individuelt

**Vurderingsformer:**

Se engelsk versjon.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Internal examiner. An external examiner is used every 4th year. Next time in the school-year 2015/2016.

**Utsatt eksamen (tidl. kontinuasjon):**

Re-sit August 2016. (Written Assignment Case Study)

**Tillatte hjelpemidler:****Obligatoriske arbeidskrav:**

Se engelsk versjon.

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Stewart Kowalski](#)

**Emneansvarlig:**

Professor Stewart Kowalski

**Klar for publisering:**

Ja

## **IMT4142 Information Security Economics 1 - 2015-2016**

**Emnekode:**

IMT4142

**Emnenavn:**

Information Security Economics 1

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Varighet (fritekst):**

Last part of Autumn semester

**Språk:**

Engelsk

**Anbefalt forkunnskap:**

IMT 4762 Risk Management 1



**Forventet læringsutbytte:**

## Knowledge

- The candidate possesses advanced knowledge about the challenges and current practices in security decision making
- The candidate possesses thorough knowledge in financial models and security metrics
- The candidate is capable of applying his/her knowledge in financial models to support security decision making

## Skills

- The candidate is able to analyze financial models and theory and apply these to security decision making situations
- The candidate is able to carry out an limited and focused security decision making process under supervision
- The candidate is able to carry out critical analysis of various literature sources on security economics and evaluate the practical implication on security decision making

## General competence

- The candidate is capable of analyzing relevant professional and research results and experiences in security economics, particularly financial models for security decision making
- The candidate is capable of applying his/her knowledge and skills in financial models to security decision making processes
- The candidate can work independently and is familiar with the challenges and current practices in security decision making
- The candidate is capable of discussing professional problems, analyses and conclusions in the field of security decision making, both with specialists and with general audience
- The candidate is capable of contributing to innovation and innovation processes

**Emnets temaer:**

1. European Unions (EU) view on information security economics
2. Current industrial practices in information security economics
3. Decision making in information security risk management
4. Financial models
5. Application of financial models as information security decision support

**Pedagogiske metoder:**

Forelesninger  
Prosjektarbeid

**Pedagogiske metoder (fritekst):**

Students are recommended to work in groups with the project. Every group must have no more than 3 members. It is also possible to complete the project individually. To ensure fairness, course deliverable grading will depend on deliverable quantity, quality and the number of contributing students.

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Muntlig, individuelt  
Vurdering av prosjekt(er)

**Vurderingsformer:**

- Project – 49%
- Oral exam (individual) – 51%
- Both parts must be passed

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Evaluated by external and internal examiner.

**Utsatt eksamen (tidl. kontinuasjon):**

For the oral exam: Re-sit August 2016

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

None

**Obligatoriske arbeidskrav:**

None

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Siv Hilde Houmb](#)

**Emneansvarlig:**

Førsteamanuensis Siv Hilde Houmb

**Læremidler:**

Books, articles and WEB resources such as

ENSIA (2008): Security Economics and the Internal Market, 114 pages. Downloadable from: [http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at\\_download/fullReport](http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport)

Anderson, R. (2001): Why Information Security is Hard - An Economic Perspective. In: ACSAC 2001: Proc. 17th Annual Computer Security Applications Conference, pages. 358–365. IEEE Press, Los Alamitos. Downloadable from: <http://www.acsac.org/2001/papers/110.pdf>

Cavusoglu, H., Cavusoglu, H. and Raghunathan, S. (2004): Economics of IT Security Management: Four Improvements to Current Security Practices. Communications of the Association for Information Systems 14, pages 65–75.

Anderson, R. J. and Moore, T. W. (2007): Information security economics – and beyond. Advances in Cryptology – Crypto 2007, LNCS 4622, Springer Verlag, Berlin Heidelberg, 68–91. Downloadable from: [http://www.cl.cam.ac.uk/rja14/Papers/econ\\_crypto.pdf](http://www.cl.cam.ac.uk/rja14/Papers/econ_crypto.pdf)

Selected parts from: Herrmann, D. S. (2007). Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resilience, and ROI. CRC Press.

Su, X. (2006). An overview of economic approaches to information security management. Downloadable from: <http://eprints.eemcs.utwente.nl/5693/01/00000177.pdf>

Daneva, M. (2006): Applying Real Options Thinking to Information Security in Networked Organizations. Tech. Rep. TR-CTIT-06-11, Centre for Telematics and Information Technology, University of Twente, Enschede. Downloadable from the website of University of Twente, NL.

Benaroch, M. and Kauffman, R.J. (1999): A Case for Using Real Options Pricing Analysis to Evaluate Information Technology Project Investment. Information Systems Research 10(1), pages 70–86.

Berthold, S. and Böhme, R. (2010): Valuating Privacy with Option Pricing Theory. In: Economics of Information Security and Privacy, pp. 187–209. Springer, Heidelberg.

Sonnenreich, W., Albanese, J., and Stout, B. (2006). Return on security investment (ROSI)-A practical quantitative model. Journal of Research and Practice in Information Technology, 38(1), pages 45-56. Downloadable from: [http://www.infosecwriters.com/text\\_resources/pdf/ROSI-Practical\\_Model.pdf](http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf)

IANS and RedSeal Networks (2011). The ROS of RedSeal. – Practical example from the industry. Downloadable from: [http://go.redsealnetworks.com/Reports\\_LP-IANS\\_ROS.html](http://go.redsealnetworks.com/Reports_LP-IANS_ROS.html)

LockStep and Australian Government Chief Information Office (GCIO) (2004). A Guide for Government Agencies Calculating Return on Security Investment. Downloadable from: <http://lockstep.com.au>

**Klar for publisering:**

Ja

## **IMT4671 Organizational and Human Aspects of Information Security - 2015-2016**

**Emnekode:**

IMT4671

**Emnenavn:**

Organizational and Human Aspects of Information Security

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Varighet (fritekst):**

Se engelsk versjon

**Språk:**

Engelsk

**Anbefalt forkunnskap:**

Se engelsk versjon.

**Forventet læringsutbytte:**

Se engelsk versjon.

**Emnets temaer:**

Se engelsk versjon.

**Pedagogiske metoder:**

Annet

**Pedagogiske metoder (fritekst):**

Termpaper with presentation at the end of the term, Readings and homework, Textbook, Powerpoint, Video-examples, Business and scientific papers, Computer Based Training, Repetition forms

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Annet

**Vurderingsformer:**

Se engelsk versjon.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Se engelsk versjon.

**Utsatt eksamen (tidl. kontinuasjon):**

Se engelsk versjon.

**Tillatte hjelpemidler:****Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Professor Bernhard M. Hämmerli

**Læremidler:**

Se engelsk versjon

**Supplerende opplysninger:**

Se engelsk versjon

**Klar for publisering:**

Ja

## IMT4722 Behavioural Biometrics - 2015-2016

**Emnekode:**

IMT4722

**Emnenavn:**

Behavioural Biometrics

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Språk:**

Engelsk

**Forventet læringsutbytte:**

Etter endt emne har studenten økt forståelse av

- ulike autentiseringsmetoder f eks passord/pin, ganglag, signatur, tastetrykk-dynamikk, tokenbaserte løsninger.
- evaluering av autentiseringsmetoder med hensyn til sikkerhetsmessig styrke

**Emnets temaer:**

- Autentisering i en sikkerhetskontekst. Hva er rimelige antagelser med hensyn på opponentens kapabiliteter.
- Utvalgte autentiseringsteknikker som f eks passord/pin, ganglag, signatur, tastetrykk-dynamikk, tokenbaserte løsninger.
- Teknikker for å evaluere autentiseringsmetoder

**Pedagogiske metoder:**

Forelesninger

Prosjektarbeid

Veiledning

**Pedagogiske metoder (fritekst):**

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Annet

**Vurderingsformer:**

Totalvurdering bestående av 100 poeng hvorav 50 poeng på prosjektarbeide og 50 poeng på avsluttende muntlig eksamen. Omregning fra 100-poengskala til A-F-skala skjer i henhold til anbefalt omregningstabell, men emneansvarlig kan i spesielle tilfeller gjøre små justeringer av grenser for å sikre overenstemmelse med de kvalitative beskrivelsene på A-F-skalaen.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Two internal sensors. An external examiner will be used every 4th year. Next time in the school-year 2017/2018.

**Utsatt eksamen (tidl. kontinuasjon):**

Ordinær kontinuasjon på skriftlig eksamen.

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Godkjent kalkulator

**Obligatoriske arbeidskrav:**

Ingen

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Patrick Bours](#)

**Emneansvarlig:**

Professor Patrick Bours

**Læremidler:**

Det eksisterer et kompendium skrevet av professoren som tildeles ved begynnelse av kurset.

**Erstatter:**

IMT5072 - Autentisering

**Supplerende opplysninger:**

In case there will be less than 5 students that will apply for the course, it will be at the discretion of Studieprogramansvarlig whether the course will be offered or not and if yes, in which form.

**Klar for publisering:**

Ja

**Emneside (URL):**

<http://www.hig.no/imt/is/courses/imt4721>

## **IMT4741 Intrusion detection and prevention - 2015-2016**

**Emnekode:**

IMT4741

**Emnenavn:**

Intrusion detection and prevention

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Varighet (fritekst):**

First half of the autumn semester

**Språk:**

Engelsk



**Forventet læringsutbytte:****Knowledge**

The candidate possesses advanced knowledge in detection and prevention of intrusions in modern computer systems and networks.

The candidate possesses thorough knowledge about theory and scientific methods relevant for intrusion detection.

The candidate is capable of applying his/her knowledge in new fields of intrusion detection and prevention.

**Skills**

The candidate is capable of analyzing existing theories, methods and interpretations in the field of intrusion detection and working independently on solving theoretical and practical problems.

The candidate can use relevant scientific methods in independent research and development in intrusion detection.

The candidate is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in the field of intrusion detection and prevention.

The candidate is capable of carrying out an independent limited research or development project in intrusion detection under supervision, following the applicable ethical rules.

**General competence**

The candidate is capable of analyzing relevant professional and research ethical problems in the field of intrusion detection.

The candidate is capable of applying his/her knowledge and skills in new fields, in order to accomplish advanced tasks and projects.

The candidate can work independently and is familiar with terminology in the field of intrusion detection and prevention.

The candidate is capable of discussing professional problems, analyses and conclusions in the field of intrusion detection and prevention, both with specialists and with general audience.

The candidate is capable of contributing to innovation and innovation processes.

**Emnets temaer:**

1. Definition and classification of IDS systems
2. Basic elements of attacks against computer networks and their detection
3. Misuse-based IDS
4. Anomaly-based IDS
5. Testing IDS and measuring their performances

**Pedagogiske metoder:**

Forelesninger  
Lab.øvelser  
Oppgaveløsning  
Prosjektarbeid

**Pedagogiske metoder (fritekst):**

Lectures

Laboratory exercises

Numerical exercises

Project work

The course will be made accessible to both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Skriftlig eksamen, 3 timer  
Vurdering av prosjekt(er)

**Vurderingsformer:**

- Written exam, 3 hours (counts 70% of the final mark)
- Project evaluation (counts 30% of the final mark)
- Both parts must be passed.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Evaluated by the lecturer. An external examiner will be used every 4th year. Next time in the school-year 2017/2018.

**Utsatt eksamen (tidl. kontinuasjon):**

Re-sit August 2016 for the written examination

**Tillatte hjelpemidler:**

D: Ingen trykte eller håndskrevne hjelpemidler tillatt. Bestemt, enkel kalkulator tillatt.

**Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Calculator, dictionary

**Obligatoriske arbeidskrav:**

None

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Slobodan Petrovic](#)

**Emneansvarlig:**

Professor Slobodan Petrovic

**Læremidler:****Compulsory literature:**

None.

**Recommended literature:**

1. Rebecca Gurley Bace, Intrusion Detection, Macmillan, 2000.
2. Jack Koziol, Intrusion Detection with SNORT, SAMS, 2003.
3. David J. Marchette, Computer Intrusion Detection and Network Monitoring - A Statistical Viewpoint, Springer Verlag, 2001.
4. Richard Bejtlich, Extrusion Detection - Security Monitoring for Internal Intrusions, Addison-Wesley, 2005.
5. Stephen Northcutt, Judy Novak, Network Intrusion Detection, 3rd edition, New Riders, 2003.

**Erstatter:**

IMT5151 - Intrusion detection and prevention

**Supplerende opplysninger:**

In case there will be less than 5 students that will apply for the course, it will be at the discretion of Studieprogramansvarlig whether the course will be offered or not and if yes, in which form.

**Klar for publisering:**

Ja

**Emneside (URL):**

<http://www.hig.no/imt/emnesider/imt4741>

## **IMT4751 Wireless communication security - 2015-2016**

**Emnekode:**

IMT4751

**Emnenavn:**

Wireless communication security

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Varighet (fritekst):**

Second half of the autumn semester

**Språk:**

Engelsk

**Forutsetter bestått:**

The student is required to have some knowledge of cryptography equivalent to IMT4532 (Cryptology 1)

**Forventet læringsutbytte:****Knowledge**

The candidate possesses advanced knowledge in the field of wireless communication security, which includes the following topics: security in RFID, wireless LAN, Bluetooth, 2G, 3G and 4G mobile telephony.

The candidate possesses thorough knowledge about theory and scientific methods relevant for wireless communication security.

The candidate is capable of applying his/her knowledge in new fields of wireless communication security.

**Skills**

The candidate is capable of analyzing existing theories, methods and interpretations in the field of wireless communication security and working independently on solving theoretical and practical problems.

The candidate can use relevant scientific methods in independent research and development in wireless communication security.

The candidate is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in the field of wireless communication security.

The candidate is capable of carrying out an independent limited research or development project in wireless communication security under supervision, following the applicable ethical rules.

**General competence**

The candidate is capable of analyzing relevant professional and research ethical problems in the field of wireless communication security.

The candidate is capable of applying his/her knowledge and skills in new fields, in order to accomplish advanced tasks and projects.

The candidate can work independently and is familiar with terminology in the field of wireless communication security.

The candidate is capable of discussing professional problems, analyses and conclusions in the field of wireless communication security, both with specialists and with general audience.

The candidate is capable of contributing to innovation and innovation processes.

**Emnets temaer:**

1. Basic radio-frequency communications
2. RFID, Wireless LAN, Bluetooth security
3. Security of 2G, 3G and 4G mobile telephony systems

**Pedagogiske metoder:**

Forelesninger

**Pedagogiske metoder (fritekst):**

Lectures

The course will be made accessible to both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Skriftlig eksamen, 3 timer

**Vurderingsformer:**

Written exam, 3 hours

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Evaluated by the lecturer. An external examiner will be used every 4th year. Next time in the school-year 2017/2018.

**Utsatt eksamen (tidl. kontinuasjon):**

Re-sit August 2016

**Tillatte hjelpemidler:**

D: Ingen trykte eller håndskrevne hjelpemidler tillatt. Bestemt, enkel kalkulator tillatt.

**Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Calculator, dictionary

**Obligatoriske arbeidskrav:**

None

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Professor Slobodan Petrovic

**Læremidler:****Books:**

1. D. Forsberg, G. Horn, W. Moeller, V. Niemi, LTE Security, 2nd. edition, Wiley, 2013.

**Erstatter:**

IMT5171 - Wireless communication security

**Supplerende opplysninger:**

In case there will be less than 5 students that will apply for the course, it will be at the discretion of Studieprogramansvarlig whether the course will be offered or not and if yes, in which form.

**Klar for publisering:**

Ja

**Emneside (URL):**

<http://www.hig.no/imt/emnesider/imt4751>

## IMT4762 Risk Management 1 - 2015-2016

**Emnekode:**

IMT4762

**Emnenavn:**

Risk Management 1

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Varighet (fritekst):**

First part of the semester

**Språk:**

Engelsk

**Forventet læringsutbytte:**

Se engelsk versjon

**Emnets temaer:**

Se engelsk versjon

**Pedagogiske metoder:**

Forelesninger

Gruppearbeid

Nettstøttet læring

Prosjektarbeid

Samling(er)/seminar(er)

Veiledning

**Pedagogiske metoder (fritekst):**

Se engelsk versjon

**Vurderingsformer:**

Muntlig, individuelt

Vurdering av prosjekt(er)

**Vurderingsformer:**

Se engelsk versjon

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Evaluated by external and internal examiner.



**Utsatt eksamen (tidl. kontinuasjon):**

Not allowed.

**Tillatte hjelpemidler:****Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Tone Hoddø Bakås](#)

**Emneansvarlig:**

Høgskolelektor Tone Hoddø Bakås

**Læremidler:**

The course literature will be the documents listed below or similar.

All literature listed below are available from ISACA ([www.isaca.org](http://www.isaca.org)).

ISACA. The Risk IT Framework. 2009. ISBN 978-1-60420-111-6

ISACA. THE RISK IT PRACTITIONER GUIDE. 2009. ISBN 978-1-60420-116-1

Additional recommended reading

IT Governance Institute. COBIT 4.1. 2007.. ISBN 1-933284-72-2

**Klar for publisering:**

Ja

## IMT4772 Risk Management 2 - 2015-2016

**Emnekode:**

IMT4772

**Emnenavn:**

Risk Management 2

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Varighet (fritekst):**

Andre halvdel av semesteret

**Språk:**

Engelsk

**Forventet læringsutbytte:**

The course contributes towards the following learning outcomes:

***Knowledge***

- Possesses advanced knowledge within the area covered by the Master Programme.
- Possesses specialized insight and good understanding of the research frontier in a selected part of the topic covered by the Master Programme.

***Skills***

- Is able to analyze existing theories, methods and interpretations and to challenge established knowledge and practice in the media technology area.
- Is able to use relevant and suitable methods when carrying out research and development activities in the area of media technologyF4: Is able to critically review relevant literature when solving new or complex problems and is able to integrate the findings into the proposed solution.
- Is able to plan and complete an independent and limited research or development project with guidance and in adherence to research ethics.

Having completed the course, the students should have:

- advanced level of understanding of assumptions and models on which risk analysis methods are based .
- deep understanding of how different assumptions/models influence outcomes of different risk analysis methods.

**Emnets temaer:**

- Classifications of Risk Management methods
- Examples of Risk Management Methods.
- Decision theory
- Risk, Threat and vulnerability discovery
- Uncertainty
- Game theory

**Pedagogiske metoder:**

Forelesninger

Oppgaveløsning

**Pedagogiske metoder (fritekst):**

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. Slides from the lectures will also be available on Internet through GUC's learning management system (Fronter).

**Vurderingsformer:**

Annet

**Vurderingsformer:**

- Written exam 3 hours (alternatively oral exam at the discretion of the course responsible): 51%
- Projects: 49%.
- Both parts must be passed.

To ensure fairness, course deliverable grading will depend on deliverable quantity, quality and the number of contributing students.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Evaluated by external and internal examiner.

**Utsatt eksamen (tidl. kontinuasjon):**

For the written exam: Re-sit August 2016

**Tillatte hjelpemidler:**

D: Ingen trykte eller håndskrevne hjelpemidler tillatt. Bestemt, enkel kalkulator tillatt.

**Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Approved calculator

**Obligatoriske arbeidskrav:**

Draft project report including scenario suitable as a basis for the other chapters. The draft report must be submitted via Fronter within 10 days of the first lecture.

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Einar Snekkenes](#)

**Emneansvarlig:**

Professor Einar Snekkenes

**Læremidler:**

Books, articles and WEB resources such as

**RA method classification**

Douglas J. Landoll. The security risk assessment handbook, p. 8-15. CRC. 2005.

Bornman, G, and Labuschagne, L, 2004, A comparative framework for evaluating information security risk management methods, In proceedings of the Information Security South Africa Conference. 2004, [www.infosecsa.co.za](http://www.infosecsa.co.za)

Vorster, A. and Labuschagne, L. 2005. A framework for comparing different information security risk analysis methodologies. In Proceedings of the 2005 Annual Research Conference of the South African institute of Computer Scientists and information Technologists on IT Research in Developing Countries (White River, South Africa, September 20 - 22, 2005). ACM International Conference Proceeding Series, vol. 150. South African Institute for Computer Scientists and Information Technologists, 95-103.

ENISA. Inventory of risk assessment and risk management methods. Deliverable 1, Final version Version 1.0, 0/03/2006

Campbell and Stamp. A classification scheme for Risk Assessment Methods. Sandia Report. SAND2004-4233.

**RA method examples**

IDART (<http://www.idart.sandia.gov/method.html>)

NIST SP 800-42, p3.1 - 3.21, 4.1- 4.3, C.1-C.9

NIST SP 800-30. p8-27

OECD, "OECD Guidelines for the Security of Information Systems and Networks -- Towards a Culture of Security." Paris: OECD. July 2002. [www.oecd.org](http://www.oecd.org). P 10-12

ISO/IEC 27005:2008(E) Information technology - Security techniquees - Information security risk management

**Decision theory**

Sven Ove Hansson. Decision Theory - A brief introduction. 2005

[http://en.wikipedia.org/wiki/Newcomb%27s\\_paradox](http://en.wikipedia.org/wiki/Newcomb%27s_paradox)

[http://en.wikipedia.org/wiki/St\\_Petersburg\\_Paradox](http://en.wikipedia.org/wiki/St_Petersburg_Paradox)

Sven Ove Hansson. Fallacies of Risk

### **Risk Threat and Vulnerability discovery**

ISO 27005, Annex C,D

Ed Yourdon. Just enough Structured Analysis. Chapter 9, Dataflow diagrams. + 'How to'.

The vulnerability assessment and mitigation methodology. Chapter 1-4, p. 1-36. MITRE technical report..

### **Uncertainty**

Lindley, Dennis V. (2006-09-11). Understanding Uncertainty. Wiley-Interscience. ISBN 978-0470043837

H. Campbell. Risk assessment: subjective or objective? Engineering science and education journal, 7:57 -63, 1998.

F. Redmill. Risk analysis-a subjective process? Engineering Management Journal. Apr 2002. Volume: 12, Issue: 2. p. 91-96

### **Game theory**

Stanford Encyclopedia of Philosophy . Game theory. Available from <http://plato.stanford.edu/entries/game-theory/>

Fudenberg, Drew & Tirole, Jean (1991), Game theory, MIT Press, ISBN 978-0-262-06141-4 , Chapters 1,3,6,8

### **Erstatter:**

IMT4771

### **Supplerende opplysninger:**

There is room for 50 students for the course.

### **Klar for publisering:**

Ja

## IMT4881 Specialization Course 1 - 2015-2016

**Emnekode:**

IMT4881

**Emnenavn:**

Specialization Course 1

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

Vår

**Varighet (fritekst):**

Can run any time during the full year.

**Språk:**

Engelsk

**Forutsetter bestått:**

Must be determined by the supervisor based upon the particular assignment.

**Forventet læringsutbytte:**

See english version

**Emnets temaer:**

The student and the supervisor will agree on a topic together. The supervisor is responsible for the fact that the workload for the student should be equivalent to other 5ECTS courses. The student will work as much as possible independently with some supervision by the supervisor.

**Pedagogiske metoder:**

Annet

**Pedagogiske metoder (fritekst):**

The teaching methods depend on the particular topic agreed upon by the student and the supervisor. There will be one mandatory meeting at the beginning of the semester. Students taking this course must participate in this session.

**Vurderingsformer:**

Vurdering av prosjekt(er)

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

External and internal examiner.

**Utsatt eksamen (tidl. kontinuasjon):**

The whole subject must be repeated.

**Tillatte hjelpemidler:****Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Patrick Bours](#)

**Emneansvarlig:**

Professor Patrick Bours

**Læremidler:**

Depending on the particular agreed upon topic

**Supplerende opplysninger:**

This course is intended for students who want to work independently on a particular topic of his/her interest. The student needs to find a supervisor by him/herself. The supervisor and the student will need to agree on a topic together. Topics can be for example (list is not exclusive):

- \* studying a particular topic from literature
- \* investigating a particular open research problem
- \* performing experiments on a research topic

In general the student will write a report on his studies or findings that can be evaluated either by the supervisor or by an external examiner. Another option for the evaluation could be writing an article for a publication or a presentation at a conference or an oral exam with the supervisor or a third person.

Students are not allowed to take both IMT4881 Specialization course 5 ECTS and IMT4882 Specialization course II 10 ECTS (either IMT4881 or IMT4882).

**Klar for publisering:**

Ja

## IMT4882 Specialization Course 2 - 2015-2016

**Emnekode:**

IMT4882

**Emnenavn:**

Specialization Course 2

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

10

**Varighet:**

Høst

Vår

**Varighet (fritekst):**

Can run any time during the full year.

**Språk:**

Engelsk

**Forutsetter bestått:**

Must be determined by the supervisor based upon the particular assignment.

**Forventet læringsutbytte:**

The student will learn how to master a particular topic individually

**Emnets temaer:**

The student and the supervisor will agree on a topic together. The supervisor is responsible for the fact that the workload for the student should be equivalent to a 10 ECTS course. The student will work as much as possible independently with some supervision by the supervisor.

**Pedagogiske metoder:**

Annet

**Pedagogiske metoder (fritekst):**

See english version

**Vurderingsformer:**

Vurdering av prosjekt(er)

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

External and internal examiner.

**Utsatt eksamen (tidl. kontinuasjon):**

The whole course must be repeated.



**Tillatte hjelpemidler:****Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Førsteamanuensis Patrick Bours

**Læremidler:**

Depending on the particular agreed upon topic

**Supplerende opplysninger:**

This course is intended for students who want to work independently on a particular topic of his/her interest. The student needs to find a supervisor by him/herself. The supervisor and the student will need to agree on a topic together. Topics can be for example (list is not exclusive):

- \* studying a particular topic from literature
- \* investigating a particular open research problem
- \* performing experiments on a research topic

In general the student will write a report on his studies or findings that can be evaluated either by the supervisor or by an external examiner. Another option for the evaluation could be writing an article for a publication or a presentation at a conference or an oral exam with the supervisor or a third person.

Students are not allowed to take both IMT4881 Specialization course 5 ECTS and IMT4882 Specialization course II 10 ECTS (either IMT4881 or IMT4882).

**Klar for publisering:**

Ja

## IMT4541 Foundations of Information Security - 2013-2014

**Emnekode:**

IMT4541

**Emnenavn:**

Foundations of Information Security

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Vår

**Språk:**

Engelsk

**Forventet læringsutbytte:****Knowledge**

- Candidates are expected to possess in-depth knowledge of modelling techniques for secure computer systems
- Candidates should have thorough knowledge of models and mechanisms for identification and authentication mechanisms
- Candidates are capable of applying methods for security analysis to novel domains in a rigorous and systematic way

**Skills**

- Candidates are expected to be capable of identifying suitable modelling techniques for analysing security requirements
- Candidates are able to undertake a research study based in part on primary literature, formulating a concise and reasoned review of such literature in the form of a structured article
- Candidates are able to apply relevant scientific methods in security modelling and analysis

**General Competence**

- Candidates are able to understand and analyze the professional, ethical, and privacy-related problems arising from the design and implementation of security models and mechanisms
- Candidates are familiar with terminology and concepts in security modelling and analysis and selected areas of information security, permitting independent work in the area
- Candidates are capable of contributing to innovation and innovation processes in information security
- Candidates are capable of discussing information security problems, particularly related to identification and authentication and security models with a specialist and also general audience.

**Emnets temaer:**

- Identification and authentication mechanisms
- Access control models and formalisms
- Decidability results and limitations of access controls and security models
- Security models, including the Bell-LaPadula, role-based access control, and Chinese Wall models
- Information theoretic models of information flow and covert channels
- Developmental assurance and evaluation criteria (optional)

**Pedagogiske metoder:**

Forelesninger

Annet

**Pedagogiske metoder (fritekst):**

- Lectures
- Tutorials
- Term paper

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Annet

**Vurderingsformer:**

- Assessment consists of two parts, pass decision is on cumulative grade of both parts:
  - Part 1 is a written examination (3 hours), accounting for 67% of grade.  
Internal and external examiners.
  - Part 2 is a term paper, accounting for 33% of grade.  
Term paper is evaluated by the lecturer.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Evaluated by external and internal examiner.

**Utsatt eksamen (tidl. kontinuasjon):**

A new term paper must be provided and the examination must be re-sat.

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Dictionary, simple calculator

**Obligatoriske arbeidskrav:**

None

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Professor Stephen Wolthusen

**Læremidler:**

The following textbooks are the primary references; further recommended reading is provided in the course syllabus.

- M. Bishop: Computer Security: Art and Science. Addison-Wesley, 2003.
- D. Gollmann: Computer Security, 2nd edition Wiley, 2006
- R. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, Chichester, UK (2001)
- A. K. Jain, P. J. Flynn, and A. A. Ross: Handbook of Biometrics. Springer-Verlag, Berlin, Germany (2007)

**Erstatter:**

IMT4162 Information Security and Security Architecture

**Klar for publisering:**

Ja

## **IMT4552 Cryptology 2 - 2013-2014**

**Emnekode:**

IMT4552

**Emnenavn:**

Cryptology 2

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Vår

**Varighet (fritekst):**

First half of the spring semester

**Språk:**

Engelsk

**Forutsetter bestått:**

IMT4532 Cryptology 1

**Forventet læringsutbytte:****Knowledge**

- The candidate possesses advanced knowledge in generating primitive feedback polynomials for application in stream ciphers based on linear feedback shift registers, constructing highly non-linear S-boxes for application in block ciphers, linear and differential cryptanalysis of block ciphers as well as primality testing, factoring large integers and discrete logarithm.
- The candidate possesses thorough knowledge about theory and scientific methods relevant for cryptology.
- The candidate is capable of applying his/her knowledge in new fields of cryptology.

**Skills**

- The candidate is capable of analyzing existing theories, methods and interpretations in the field of cryptology and working independently on solving theoretical and practical problems.
- The candidate can use relevant scientific methods in independent research and development in cryptology.
- The candidate is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in cryptology.
- The candidate is capable of carrying out an independent limited research or development project in cryptology under supervision, following the applicable ethical rules.

**General competence**

- The candidate is capable of analyzing relevant professional and research ethical problems in cryptology.
- The candidate is capable of applying his/her cryptographic knowledge and skills in new fields, in order to accomplish advanced tasks and projects.
- The candidate can work independently and is familiar with cryptographic terminology.
- The candidate is capable of discussing professional problems, analyses and conclusions in the field of cryptology, both with specialists and with general audience.
- The candidate is capable of contributing to innovation and innovation processes.

**Emnets temaer:**

1. Stream ciphers
2. Block ciphers
3. Public key ciphers with applications.

**Pedagogiske metoder:**

Forelesninger  
Oppgaveløsning  
Prosjektarbeid

**Pedagogiske metoder (fritekst):**

Lectures

Numerical exercises

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

Project work

**Vurderingsformer:**

Skriftlig eksamen, 3 timer

Vurdering av prosjekt(er)

**Vurderingsformer:**

Written exam, 3 hours, counts for 70% of the final mark

Project work, counts for 30% of the final mark

Both exam and project must be passed

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Evaluated by the lecturer. An external examiner will be used every 4th year. Next time in the school-year 2014/2015.

**Utsatt eksamen (tidl. kontinuasjon):**

Ordinary re-sit examination. The project work (if passed) need not be repeated.

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Calculator, dictionary

**Obligatoriske arbeidskrav:**

None

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Professor Slobodan Petrovic

**Læremidler:****Books:**

1. Introduction to Cryptography and Coding Theory, 2. edition, Trappe W., Washington L., Prentice Hall, 2006, ISBN: 0131981994.

2. Handbook of Applied Cryptography, Menezes A., <http://www.cacr.math.uwaterloo.ca/hac>

**Erstatter:**

IMT4551 Selected Topics in Cryptology

**Klar for publisering:**

Ja

**Emneside (URL):**

<http://www.hig.no/imt/emnesider/imt4552>



## **IMT4621 Biometrics - 2013-2014**

**Emnekode:**

IMT4621

**Emnenavn:**

Biometrics

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Vår

**Varighet (fritekst):**

First half of spring semester

**Språk:**

Engelsk

**Anbefalt forkunnskap:**

The course content will be complementary to the course IMT4721 "Authentication".

**Forventet læringsutbytte:****Knowledge:**

- The candidate possesses advanced knowledge in Biometrics.
- The candidate possesses thorough knowledge about theory and scientific methods relevant for design, development and operation of biometric access control systems.
- The candidate is capable of applying his/her knowledge in new fields of IT-security systems.

**Skills**

- The candidate is capable of analyzing existing theories, methods and interpretations in the field of biometrics and working independently on solving theoretical and practical problems.
- The candidate can use relevant scientific methods in independent research and development in biometrics.
- The candidate is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in biometrics.
- The candidate is capable of carrying out an independent limited research or development project in biometrics under supervision, following the applicable ethical rules.

**General competence**

- The candidate is capable of analyzing relevant professional and research ethical problems in biometrics.
- The candidate is capable of applying his/her biometric knowledge and skills in new fields, in order to accomplish advanced tasks and projects.
- The candidate can work independently and is familiar with biometric terminology.
- The candidate is capable of discussing professional problems, analyses and conclusions in the field of biometrics, both with specialists and with general audience.
- The candidate is capable of contributing to innovation and innovation processes.

**Objectives:**

After the course, the students should have acquired:

1. Knowledge about common statistical tools for biometrics
2. Insight into advantages and disadvantages of biometric characteristics
3. Understanding of multimodal biometrics
4. Knowledge of ethical and privacy issues in biometrics.
5. Understanding of the threats and protection mechanisms for biometric data.

**Emnets temaer:  
Content**

In this course, several key aspects of biometrics are covered. The course begins with an overview of applied statistics and hypothesis tests as well as other common statistical tools for biometrics, and then covers selected biometric concepts, particularly fingerprint recognition, vein recognition, face recognition and iris recognition. To this end, the relevant physiological characteristics, their variability, and potential problems are discussed before analyzing different approaches for each of the attributes to be investigated. In each case, not only benign applications are covered but also potential bottlenecks such as insufficient sample quality along the entire processing chain. The use of multi-biometrics including data fusion is discussed both in the context of robustness against attacks and improving the overall accuracy of the recognition process. The course continues with a discussion of the ethical and privacy-related issues in biometrics, along with possible limitations and technical mitigation mechanisms. Special attention is given to privacy enhancing technologies that provides protection of sensitive biometric data. In this line the course concludes with comparison-on-card approaches and template protection concepts that allow revocation of biometric references.

**Key Topics:**

- Fingerprint recognition
- Vein recognition
- Face recognition
- Iris recognition
- Multimodal biometrics
- Attack mechanisms
- Privacy Enhancing Technologies

**Pedagogiske metoder:**

Annet

**Pedagogiske metoder (fritekst):****Tutorial:**

Afternoon sessions with seminar discussion and practical tasks.

**Assignment:**

Students should provide a research report (term paper) on a topic that is chosen by the student in coordination with the lecturer.

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Annet

**Vurderingsformer:**

1. If the student decides to conduct a term paper the grading will be based on two elements with the following weighting:

- Written examination in English (3 hours): 67%
- Term paper and oral presentation of term paper results: 33%.
- Both parts of the assessment have to be passed to pass the course.

2. Otherwise the final exam will be weighted 100%.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Written exam will be graded by an external examiner.

Term paper and oral presentation will be graded by an internal examiner

**Utsatt eksamen (tidl. kontinuasjon):**

Ordinary re-sit examination.

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Dictionaries allowed (no calculator)

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Professor Christoph Busch

**Læremidler:****Recommended literature:**

[1] LI, S. Z., AND JAIN, A. K., Eds. Handbook of Face Recognition. Springer, Heidelberg, Germany, 2011.

[2] MALTONI, D., MAIO, D., JAIN, A. K., AND PRABHAKAR, S. Handbook of Fingerprint Recognition. Springer, 2009.

[3] WAYMAN, J., JAIN, A., MALTONI, D., AND MAIO, D., Biometric Systems. Springer, 2005.

[4] JAIN, L.C., HALICI, U., HAYASHI, I.; LEE, S.B., TSUTSUI, S. Intelligent Biometric Techniques in Fingerprint and Face Recognition. CRC Press, 1999.

[5] TUYLS, P., SKROIC, B., KEVENAAR, T. Security with Noisy Data. Springer, 2007

**Supplerende opplysninger:**

In case there will be less than 5 students that will apply for the course, it will be at the discretion of Studieprogramansvarlig whether the course will be offered or not and if yes, in which form.

**Klar for publisering:**

Ja

## IMT4122 Software Security Trends - 2013-2014

**Emnekode:**

IMT4122

**Emnenavn:**

Software Security Trends

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Vår

**Språk:**

Engelsk

**Anbefalt forkunnskap:**

Se engelsk versjon

**Forventet læringsutbytte:**

Se engelsk versjon

**Emnets temaer:**

Se engelsk versjon

**Pedagogiske metoder:**

Forelesninger

Lab.øvelser

PBL (Problem Basert Læring)

Prosjektarbeid

**Vurderingsformer:**

Vurdering av prosjekt(er)

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Se engelsk versjon

**Utsatt eksamen (tidl. kontinuasjon):**

Se engelsk versjon

**Tillatte hjelpemidler:****Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Førsteamanuensis Hanno Langweg

**Læremidler:**

Se engelsk versjon

**Klar for publisering:**

Ja

## IMT4571 IT Governance - 2014-2015

**Emnekode:**

IMT4571

**Emnenavn:**

IT Governance

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Varighet (fritekst):**

Andre halvdel av semesteret

**Språk:**

Engelsk



## Forventet læringsutbytte:

### Knowledge

- The candidate possesses detailed knowledge of IT Governance principles and procedures, and the basic concepts of the ISO 27001 / ISO 27002 (2005) standard.
- The candidate possesses thorough knowledge about the overall process for establishment and maintenance of an Information Security Management Systems (ISMS).
- The candidate possesses detailed knowledge about the role of policies, standards and guidelines for controls and is capable of applying his/her knowledge in case studies.

### Skills

- The candidate is capable of applying IT Governance principles on practical case-studies, including proposal and evaluation of technical security architectures and solutions.
- The candidate is capable of performing stakeholder analysis, risk assessment and recommending risk treatment plans on limited case-studies.
- The candidate is capable of evaluating the applicability of common security mechanism for various controls given a certain scope and policy for the control.

### General competence

- The candidate is capable of analyzing business and organizational needs for an ISMS and has a thorough understanding of security management as a continuous improvement process.
- The candidate can work independently and is familiar with IT Governance terminology.
- The candidate is capable of discussing professional problems such as documentation, decision making processes, implementation plans, operations, reviews and corrective actions, with both IT specialists and general managers.

**Emnets temaer:**

- Reasons for IT Governance: Compliance, liability, stability
- Organizing information security
- Information security policy and scope
- The risk assessment and statement of applicability
- Identification of risks related to external parties
- Asset management
- Human resources security
- Physical and environmental security
- Equipment security
- Communications and operations management
- Controls against malicious software (malware) and back-ups
- Network security management and media handling
- Exchanges of information
- Electronic commerce services
- E-mail and internet use
- Access control
- Network access control
- Operating system access control
- Application access control and teleworking
- Systems acquisition, development and maintenance
- Cryptographic controls
- Security in development and support processes
- Monitoring and information security incident management
- Business continuity management
- Compliance
- Principles of auditing

**Pedagogiske metoder:**

Annet

**Pedagogiske metoder (fritekst):**

Lectures, exercises and projects.

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Annet

**Vurderingsformer:**

- 1-2 Multiple Choice Tests (weight: 20%)
- 1-2 group Assignments (weight: 30%)
- Digital Final exam, 2 hours (weight: 50%)

The final digital exam is conducted in Fronter with students present in the computer lab at HiG  
All three parts are mandatory and must be passed!

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Evaluated by the lecturer. An external examiner will be used every 4th year. Next time in the school-year 2014/2015.

**Utsatt eksamen (tidl. kontinuasjon):**

For the final exam: Ordinary re-sit examination.

**Tillatte hjelpemidler:****Obligatoriske arbeidskrav:**

None.

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

Åsmund Skomedal

**Emneansvarlig:**

Forskningssjef Åsmund Skomedal

**Læremidler:**

Literature:

Alan Calder & Steve Watkins. IT Governance : An International Guide to Data Security and ISO 27001 / ISO 27002. Fifth Edition. Kogan Page. 2012.

Anderson, Ross (1999) Why cryptosystems fail, University Computer Laboratory, University of Cambridge, Cambridge, UK, <http://www.cl.cam.ac.uk/~rja14/wcf.html>.

**Klar for publisering:**

Ja

## IMT4591 Legal Aspects of Information Security - 2014-2015

**Emnekode:**

IMT4591

**Emnenavn:**

Legal Aspects of Information Security

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Varighet (fritekst):**

Første del av høstsemester

**Språk:**

Norsk, alternativt engelsk

**Forventet læringsutbytte:*****Knowledge***

- The candidate possesses advanced knowledge in legal aspects especially relevant for information security. This applies particularly to the legal regulation of matters of importance to safeguarding confidentiality, integrity, access and quality.

***Skills***

- The candidate is capable of performing critical analysis of various literature sources regarding legal aspects of information security.
- The candidate is capable of carrying out an independent limited research or development project in legal aspects of information security under supervision, following the applicable ethical rules.

***General competence***

- The candidate is capable of analyzing relevant professional and research ethical problems in legal aspects of information security.
- The candidate is capable of applying his/her knowledge about legal aspects of information security in new fields, in order to accomplish advanced tasks and projects.
- The candidate can work independently and is familiar with legal terminology.

**Emnets temaer:**

Generelle bestemmelser om informasjonssikkerhet, særlig innenfor e-forvaltning

Sikring av personopplysninger ved innsamling, bearbeiding og lagring av opplysninger

Regler for elektronisk kommunikasjon

**Pedagogiske metoder:**

Forelesninger  
Gruppearbeid  
Oppgaveløsning  
Samling(er)/seminar(er)

**Pedagogiske metoder (fritekst):**

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (Fronter).

**Vurderingsformer:**

Skriftlig eksamen, 3 timer

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Intern + ekstern sensor

**Utsatt eksamen (tidl. kontinuasjon):**

Ingen ordinær kontinuasjon

**Tillatte hjelpemidler:****Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Lise Nilsen](#)

**Emneansvarlig:**

Timelærer Lise Nilsen

**Læremidler:**

Se oversikt i emnets rom i Fronter.

**Klar for publisering:**

Ja

## IMT4122 Software Security Trends - 2014-2015

**Emnekode:**

IMT4122

**Emnenavn:**

Software Security Trends

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Vår

**Språk:**

Engelsk

**Anbefalt forkunnskap:**

Se engelsk versjon

**Forventet læringsutbytte:**

Se engelsk versjon

**Emnets temaer:**

Se engelsk versjon

**Pedagogiske metoder:**

Forelesninger

Lab.øvelser

PBL (Problem Basert Læring)

Prosjektarbeid

**Vurderingsformer:**

Vurdering av prosjekt(er)

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Se engelsk versjon

**Utsatt eksamen (tidl. kontinuasjon):**

Se engelsk versjon

**Tillatte hjelpemidler:****Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Hanno Langweg](#)

**Emneansvarlig:**

Førsteamanuensis Hanno Langweg

**Læremidler:**

Se engelsk versjon

**Klar for publisering:**

Ja

## IMT4621 Biometrics - 2014-2015

**Emnekode:**

IMT4621

**Emnenavn:**

Biometrics

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Vår

**Varighet (fritekst):**

First half of spring semester

**Språk:**

Engelsk

**Anbefalt forkunnskap:**

The course content will be complementary to the course IMT4721 "Authentication".



**Forventet læringsutbytte:****Knowledge:**

- The candidate possesses advanced knowledge in Biometrics.
- The candidate possesses thorough knowledge about theory and scientific methods relevant for design, development and operation of biometric access control systems.
- The candidate is capable of applying his/her knowledge in new fields of IT-security systems.

**Skills**

- The candidate is capable of analyzing existing theories, methods and interpretations in the field of biometrics and working independently on solving theoretical and practical problems.
- The candidate can use relevant scientific methods in independent research and development in biometrics.
- The candidate is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in biometrics.
- The candidate is capable of carrying out an independent limited research or development project in biometrics under supervision, following the applicable ethical rules.

**General competence**

- The candidate is capable of analyzing relevant professional and research ethical problems in biometrics.
- The candidate is capable of applying his/her biometric knowledge and skills in new fields, in order to accomplish advanced tasks and projects.
- The candidate can work independently and is familiar with biometric terminology.
- The candidate is capable of discussing professional problems, analyses and conclusions in the field of biometrics, both with specialists and with general audience.
- The candidate is capable of contributing to innovation and innovation processes.

**Objectives:**

After the course, the students should have acquired:

1. Knowledge about common statistical tools for biometrics
2. Insight into advantages and disadvantages of biometric characteristics
3. Understanding of multimodal biometrics
4. Knowledge of ethical and privacy issues in biometrics.
5. Understanding of the threats and protection mechanisms for biometric data.

**Emnets temaer:  
Content**

In this course, several key aspects of biometrics are covered. The course begins with an overview of applied statistics and hypothesis tests as well as other common statistical tools for biometrics, and then covers selected biometric concepts, particularly fingerprint recognition, vein recognition, face recognition and iris recognition. To this end, the relevant physiological characteristics, their variability, and potential problems are discussed before analyzing different approaches for each of the attributes to be investigated. In each case, not only benign applications are covered but also potential bottlenecks such as insufficient sample quality along the entire processing chain. The use of multi-biometrics including data fusion is discussed both in the context of robustness against attacks and improving the overall accuracy of the recognition process. The course continues with a discussion of the ethical and privacy-related issues in biometrics, along with possible limitations and technical mitigation mechanisms. Special attention is given to privacy enhancing technologies that provides protection of sensitive biometric data. In this line the course concludes with comparison-on-card approaches and template protection concepts that allow revocation of biometric references.

**Key Topics:**

- Fingerprint recognition
- Vein recognition
- Face recognition
- Iris recognition
- Multimodal biometrics
- Attack mechanisms
- Privacy Enhancing Technologies

**Pedagogiske metoder:**

Annet

**Pedagogiske metoder (fritekst):****Tutorial:**

Afternoon sessions with seminar discussion and practical tasks.

**Assignment:**

Students should provide a research report (term paper) on a topic that is chosen by the student in coordination with the lecturer.

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Annet

**Vurderingsformer:**

1. If the student decides to conduct a term paper the grading will be based on two elements with the following weighting:

- Written examination in English (3 hours): 67%
- Term paper and oral presentation of term paper results: 33%.
- Both parts of the assessment have to be passed to pass the course.

2. Otherwise the final exam will be weighted 100%.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Written exam will be graded by an external examiner.

Term paper and oral presentation will be graded by an internal examiner

**Utsatt eksamen (tidl. kontinuasjon):**

No re-sit examination offered.

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Dictionaries allowed (no calculator)

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Christoph Busch](#)

**Emneansvarlig:**

Professor Christoph Busch

**Læremidler:****Recommended literature:**

[1] LI, S. Z., AND JAIN, A. K., Eds. Handbook of Face Recognition. Springer, Heidelberg, Germany, 2011.

[2] MALTONI, D., MAIO, D., JAIN, A. K., AND PRABHAKAR, S. Handbook of Fingerprint Recognition. Springer, 2009.

[3] WAYMAN, J., JAIN, A., MALTONI, D., AND MAIO, D., Biometric Systems. Springer, 2005.

[4] JAIN, L.C., HALICI, U., HAYASHI, I.; LEE, S.B., TSUTSUI, S. Intelligent Biometric Techniques in Fingerprint and Face Recognition. CRC Press, 1999.

[5] TUYLS, P., SKROIC, B., KEVENAAR, T. Security with Noisy Data. Springer, 2007

**Supplerende opplysninger:**

In case there will be less than 5 students that will apply for the course, it will be at the discretion of Studieprogramansvarlig whether the course will be offered or not and if yes, in which form.

**Klar for publisering:**

Ja

## IMT4601 Research Project Planning - 2015-2016

**Emnekode:**

IMT4601

**Emnenavn:**

Research Project Planning

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

Vår

**Varighet (fritekst):**

See English version

**Språk:**

Engelsk

**Forutsetter bestått:**

IMT4421 Scientific Methodology or

IMT4192 Research and Scientific Methods in HCI

**Forventet læringsutbytte:**

See English version

**Emnets temaer:**

See English version

**Pedagogiske metoder:**

Forelesninger

**Pedagogiske metoder (fritekst):**

See English version

**Vurderingsformer:**

Vurdering av prosjekt(er)

**Vurderingsformer:**

See English version

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

See English version

**Utsatt eksamen (tidl. kontinuasjon):**

See English version

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

See English version

**Obligatoriske arbeidskrav:**

See English version

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Einar Snekkenes](#)

**Emneansvarlig:**

Professor Einar Snekkenes

**Læremidler:**

See English version

**Supplerende opplysninger:**

See English version

**Klar for publisering:**

Ja

**Emneside (URL):**

<http://www.hig.no/imt/emnesider/imt4601>

## IMT4904 Master Thesis - 2015-2016

**Emnekode:**

IMT4904

**Emnenavn:**

Master Thesis

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

30

**Varighet:**

Høst

Vår

**Varighet (fritekst):**

Se engelsk beskrivelse.

**Gjelder fra vårsemesteret 2013.****Språk:**

Norsk, alternativt engelsk

**Forutsetter bestått:**

Se engelsk beskrivelse.

**Forventet læringsutbytte:**

Se engelsk beskrivelse.

**Emnets temaer:**

Se engelsk beskrivelse.

**Pedagogiske metoder:**

Prosjektarbeid

Samling(er)/seminar(er)

Veiledning

**Vurderingsformer:**

Annet

**Vurderingsformer:**

Se engelsk beskrivelse.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Se engelsk beskrivelse.

**Utsatt eksamen (tidl. kontinuasjon):**

Se engelsk beskrivelse.

**Tillatte hjelpemidler:****Obligatoriske arbeidskrav:**

Se engelsk beskrivelse.

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Hilde Bakke](#)

**Emneansvarlig:**

Hilde Bakke

**Klar for publisering:**

Ja

**Emneside (URL):**

<http://www.hig.no/imt/emnesider/imt4901>



## IMT4012 Digital Forensics 1 - 2014-2015

**Emnekode:**

IMT4012

**Emnenavn:**

Digital Forensics 1

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Høst

**Språk:**

Engelsk

**Forutsetter bestått:**

se engelsk versjon

**Anbefalt forkunnskap:**

se engelsk versjon

**Forventet læringsutbytte:**

se engelsk versjon

**Emnets temaer:**

se engelsk versjon

**Pedagogiske metoder:**

Forelesninger

Lab.øvelser

Prosjektarbeid

**Vurderingsformer:**

Muntlig fremføring

Skriftlig eksamen, 3 timer

Vurdering av prosjekt(er)

**Vurderingsformer:**

se engelsk versjon

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

se engelsk versjon

**Utsatt eksamen (tidl. kontinuasjon):**

se engelsk versjon

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

se engelsk versjon

**Obligatoriske arbeidskrav:**

se engelsk versjon

**Ansvarlig avdeling:**

Avdeling for teknologi, økonomi og ledelse

**Emneansvarlig kobling:**

[Andre Årnes](#)

**Emneansvarlig:**

Associate Professor André Årnes (andre.arnes@hig.no)

**Læremidler:**

se engelsk versjon

**Supplerende opplysninger:**

se engelsk versjon

**Klar for publisering:**

Ja

## **IMT4841 Security Planning and Incident Management - 2014-2015**

**Emnekode:**

IMT4841

**Emnenavn:**

Security Planning and Incident Management

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

10

**Varighet:**

Vår

**Varighet (fritekst):**

Ett semester

**Språk:**

Norsk, alternativt engelsk

**Forventet læringsutbytte:****Kunnskap**

Studenten har etter fullført emne generell kunnskap om sikkerhetsplanlegging og hendelseshåndtering samt fordypning i ett av emnets temaer gjennom det selvstendige prosjektarbeidet.

Den generelle kunnskapen omfatter beredskapsplanlegging for håndtering av forretningskritiske hendelser. Det blir lagt vekt på både mindre hendelser og større hendelser hvor det kan være nødvendig å flytte drift til en annen lokasjon.

**Ferdigheter**

Studenten er i stand til å utarbeide beredskapsplaner for større og mindre informasjonssikkerhetshendelser.

Studenten er i stand til å lede planleggingsprosessen på en selvstendig måte.

**Generell kompetanse**

Studenten er i stand til selvstendig å fremskaffe informasjon/litteratur som omhandler sikkerhetsplanlegging og hendelseshåndtering. Videre er studenten i stand til å kritisk vurdere denne informasjonen og bruke den aktivt i beredskapsplanleggingsprosessen.

Studenten er i stand til å kommunisere overnevnte informasjon til andre.

**Emnets temaer:**

1. Introduksjon og overblikk over hendelseshåndtering beredskapsplanlegging.
2. Planlegging for en beredskapsorganisasjon: Risikostyring, risikostyringens begrensninger, hendelsesrapporteringssystemer, konsekvensanalyse
3. Hendelseshåndtering: forberedelse, organisering, preventive tiltak, deteksjon, hendelsesmelding, reaksjon, gjenoppbygging, vedlikehold, operasjonelle problemer for CSIRTs, og organisasjonsmodeller for CSIRTs.
4. Katastrofehåndtering: Forberedelse, gjennomføring, drift og vedlikehold.
5. Kontinuitetsplanlegging: Forberedelse, gjennomføring, drift og vedlikehold.
6. Krisehåndtering og menneskelige faktorer.

**Pedagogiske metoder:**

Essay  
Forelesninger  
Nettbasert Læring  
Nettstøttet læring  
Refleksjon  
Veiledning

**Pedagogiske metoder (fritekst):**

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

**Vurderingsformer:**

Skriftlig eksamen, 3 timer  
Vurdering av prosjekt(er)

**Vurderingsformer:**

Totalvurdering bestående av 100 poeng hvorav 50 poeng kan oppnåes på prosjektarbeide og 50 poeng på avsluttende 3-timers eksamen. Omregning fra 100-poengskala til A-F-skala skjer i henhold til anbefalt omregningstabell, men emneansvarlig kan i spesielle tilfeller gjøre små justeringer av grenser for å sikre overenstemmelse med de kvalitative beskrivelsene på A-F-skalaen. Både eksamen og prosjektarbeidet må bestås.

Prosjektarbeidet består av et selvstendig arbeid hvor studenten selv må fordype seg i et av emnets temaer. Studenten vil bli veiledet og motta tilbakemeldinger på arbeidet underveis.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Internal examiner. An external examiner will be used every 4th year. Next time in the school-year 2014/2015.

**Utsatt eksamen (tidl. kontinuasjon):**

Ordinær kontinuasjon på skriftlig eksamen

**Tillatte hjelpemidler:**

**Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Ordbok: Engelsk-Norsk, Norsk til annet språk eller Engelsk til annet språk.

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Marie Elisabeth Gaup Moe](#)

**Emneansvarlig:**

Associate professor II Marie Gaup Moe

**Læremidler:**

Michael Whitman, Herbert Mattord og Andrew Green: Principles of Incident Response and Disaster Recovery, 2nd edition . Thomson, 2014.

Tilleggs litteratur vil bli utdelt eller gjort tilgjengelig på Fronter.

**Erstatter:**

IMT5161 - Incident response and computer forensics

**Supplerende opplysninger:**

Dette emnet er tilpasset studenter som følger fleksible-master-programmet og som ikke er tilstede på campus. Alle forelesninger kringkastes over internett i sanntid og lagres også slik at de kan ses i etterkant. Det tas opp både bilde og lyd. Veiledningsmøter kan gjennomføres online så lenge studenten har mikrofon tilgjengelig. Et webcam anbefales også.

Emnet undervises parallelt med bacheloremnet IMT3521.

Students that have already taken course IMT3521 Introduction to security Planning and Incident Handling at bachelor level cannot apply to be exempted from taking IMT4841 Security Planning and Incident Management when studying Master in Information Security, because expected learning outcomes in both courses are different.

**Klar for publisering:**

Ja

## **IMT4612 Machine Learning and Pattern Recognition 1 - 2013-2014**

**Emnekode:**

IMT4612

**Emnenavn:**

Machine Learning and Pattern Recognition 1

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Vår

**Språk:**

Engelsk

**Anbefalt forkunnskap:**

Se engelsk versjon.

**Forventet læringsutbytte:**

Se engelsk versjon.

**Emnets temaer:**

Se engelsk versjon.

**Pedagogiske metoder:**

Forelesninger

Lab.øvelser

Nettstøttet læring

Oppgaveløsning

**Vurderingsformer:**

Skriftlig eksamen, 3 timer

Øvinger

**Vurderingsformer:**

Se engelsk versjon.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

One internal and one external examiner

**Utsatt eksamen (tidl. kontinuasjon):**

For the exam: Ordinary re-sit examination.

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

None

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Professor Katrin Franke

**Læremidler:**

Literature and study materials: Handouts of the material covered in the lectures will be distributed.

- R.O.Duda, P.E. Hart, and D.G. Storck: Pattern Classification. 2nd ed., Wiley, 2001.
- Sergios Theodoridis, Konstantinos Koutroumbas. "Pattern Recognition", third edition. Academic Press.

**Erstatter:**

IMT4611

**Supplerende opplysninger:**

In case there will be less than 5 students that will apply for the course, it will be at the discretion of Studieprogramansvarlig whether the course will be offered or not and if yes, in which form.

**Klar for publisering:**

Ja

## IMT4641 Computational Forensics - 2013-2014

**Emnekode:**

IMT4641

**Emnenavn:**

Computational Forensics

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

5

**Varighet:**

Vår

**Varighet (fritekst):**

Andre halvdel av semesteret

**Språk:**

Engelsk

**Forventet læringsutbytte:**

Se engelsk versjon

**Emnets temaer:**

Se engelsk versjon

**Pedagogiske metoder:**

Prosjektarbeid

**Pedagogiske metoder (fritekst):**

Se engelsk versjon

**Vurderingsformer:**

Vurdering av prosjekt(er)

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Se engelsk versjon

**Utsatt eksamen (tidl. kontinuasjon):**

Se engelsk versjon

**Tillatte hjelpemidler:****Obligatoriske arbeidskrav:**

None.



**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Professor Katrin Franke

**Læremidler:**

Se engelsk versjon

**Supplerende opplysninger:**

Se engelsk versjon

**Klar for publisering:**

Ja

## IMT4022 Digital Forensics 2 - 2013-2014

**Emnekode:**

IMT4022

**Emnenavn:**

Digital Forensics 2

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

10

**Varighet:**

Vår

**Språk:**

Engelsk

**Forutsetter bestått:**

se engelsk versjon

**Anbefalt forkunnskap:**

se engelsk versjon

**Forventet læringsutbytte:**

se engelsk versjon

**Emnets temaer:**

se engelsk versjon

**Pedagogiske metoder:**

Forelesninger

Lab.øvelser

**Vurderingsformer:**

Annet

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

se engelsk versjon

**Utsatt eksamen (tidl. kontinuasjon):**

se engelsk versjon

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

se engelsk versjon

**Obligatoriske arbeidskrav:**

se engelsk versjon

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig:**

Professor Katrin Franke (katrin.franke@hig.no) /Adjunct Associate Professor André Årnes  
(andre.arnes@hig.no)

**Læremidler:**

se engelsk versjon

**Supplerende opplysninger:**

se engelsk versjon

**Klar for publisering:**

Ja

## IMT4022 Digital Forensics 2 - 2014-2015

**Emnekode:**

IMT4022

**Emnenavn:**

Digital Forensics 2

**Faglig nivå:**

Master (syklus 2)

**Studiepoeng:**

10

**Varighet:**

Vår

**Språk:**

Engelsk

**Forutsetter bestått:**

Se engelsk versjon.

**Anbefalt forkunnskap:**

Se engelsk versjon.

**Forventet læringsutbytte:**

Se engelsk versjon.

**Emnets temaer:**

Se engelsk versjon.

**Pedagogiske metoder:**

Essay

Forelesninger

Lab.øvelser

Oppgaveløsning

Prosjektarbeid

**Pedagogiske metoder (fritekst):**

Se engelsk versjon.

**Vurderingsformer:**

Skriftlig eksamen, 3 timer

Vurdering av prosjekt(er)

**Vurderingsformer:**

Se engelsk versjon.

**Karakterskala:**

Bokstavkarakterer, A (best) - F (ikke bestått)

**Sensorordning:**

Se engelsk versjon.

**Utsatt eksamen (tidl. kontinuasjon):**

Se engelsk versjon.

**Tillatte hjelpemidler:****Tillatte hjelpemidler (gjelder kun skriftlig eksamen):**

Se engelsk versjon.

**Obligatoriske arbeidskrav:**

Se engelsk versjon.

**Ansvarlig avdeling:**

Avdeling for informatikk og medieteknikk

**Emneansvarlig kobling:**

[Katrin Franke](#)

**Emneansvarlig:**

Professor Katrin Franke (katrin.franke@hig.no) / Adjunct Associate Professor André Årnes (andre.arnes@hig.no)

**Læremidler:**

Se engelsk versjon.

**Supplerende opplysninger:**

Se engelsk versjon.

**Klar for publisering:**

Ja