AALBORG UNIVERSITET

STUDIEORDNING FOR MASTERUDDANNELSEN I CYBERSIKKERHED OG PRIVACY, 2022

MASTER
KØBENHAVN

MODULER SOM INDGÅR I STUDIEORDNINGEN

INDHOLDSFORTEGNELSE

SECURITY AND PRIVACY IN ORGANISATIONAL SYSTEMS

2023/2024

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

The objective is to give the course participants knowledge, skills and competencies to be able to analyse a selected company IT system, focusing on either security or privacy weaknesses.

Furthermore, the project contains a small module on Problem Based Learning (PBL) and Scientific methods.

LEARNING OBJECTIVES

KNOWLEDGE

- Must have knowledge about security and privacy weaknesses and vulnerability in the company IT systems
- Must have knowledge about risks and risk assessment in organisational systems
- Must have knowledge about basic principals in PBL and POPBL
- Must have knowledge about scientific methods relevant for the education

SKILLS

- Must be able to use the methods and theories from the courses in the trimester on specific company cases
- Must be able to create a plan for testing a selected system and assessing methods for eliminating the vulnerabilities

COMPETENCES

- Must have competencies to asses security and privacy vulnerabilities in the organisational systems and identify cyber security and privacy needs of an organization
- Must have competencies to analyse a specific case, identify vulnerabilities and come up with a mitigation plan/strategy
- Must have the competency to assess and select relevant scientific and technical literature within the various subject areas of cyber security and privacy
- Must have competencies to work in groups and to write an academic report using relevant scientific methods.

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Security and Privacy in Organisational Systems
Type of exam	Oral exam based on a project
ECTS	10
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Sikkerhed og privacy i organisatoriske systemer
Module code	ESNMCSPM1P1
Module type	Project
Duration	1 semester
Semester	Autumn
ECTS	10
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Education owner	Master of Cyber Security and Privacy
Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	The Technical Faculty of IT and Design

APPLICATION AND NETWORK SECURITY

2023/2024

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

The aim of the course is to give the fundamentals theories, methods and principles related to application and network security

LEARNING OBJECTIVES

KNOWLEDGE

- Must have knowledge about basic concepts about application and network security
- Must have knowledge about the CIA model (confidentiality, integrity and availability) and what that means for security and privacy
- Must have knowledge about Network security threats
- Must have knowledge about vulnerabilities and attack methods and the function and application of the network components and applications used for countering threats
- Must have knowledge about methods for authentication of people, network traffic and systems in the covered protocols and applications
- Must have knowledge about access management systems and technologies

SKILLS

- Must have the ability to consider cyber security issues in IT systems
- Must have the ability to identify typical content and best practices in a company’s security policy
- Must be able to apply state-of-the-art technologies for realising advanced services with access control

COMPETENCES

- Must have competencies to identify security weaknesses on an IT system analysing the basics of the architecture and its protocols

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Application and Network Security
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Applikation og netværk sikkerhed

Module code	ESNMCSPM1K1
Module type	Course
Duration	1 semester
Semester	Autumn
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Education owner	Master of Cyber Security and Privacy
Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	The Technical Faculty of IT and Design

DATA PROTECTION AND PRIVACY

2023/2024

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

The course gives the participants theoretical knowledge with privacy and data protection and different methods and theories to use for analysis. Methods for mitigation includes a combination of technological solutions, laws and regulations, and user adapted behavior (Kahneman's theory). Ethical perspectives of the data processing are discussed and can be used to set a sort of risk level to how the data processes are handled.

LEARNING OBJECTIVES

KNOWLEDGE

- Must have knowledge about basic concepts about data protection and privacy
- Must have knowledge about Privacy as a concept and how it can change with the focus of technical, organisation, user and ethical
- Must have knowledge about legal problems and measures to prevent and diminish problems within: Personal data and other related information on privacy; intellectual property rights; protecting business secrets; net and information security and criminal cyberattacks
- Must have knowledge about Data protection and ethical perspectives of data protection
- Must have knowledge about Privacy theories and models
- Must have knowledge about the concept of privacy engineering and its different perspectives and areas of expertise
- Must have knowledge about examples of systems and emerging technologies and how they challenge privacy and data protection

SKILLS

- Must have the ability to consider privacy issues in IT systems
- Must have the ability to identify data protection acts in a selected IT-System and discuss what the impacts are on the system
- Must have the ability to do a data risk analysis of selected emerging technologies
- Must have the ability to see data protection and privacy from an ethical angle

COMPETENCES

- Must have competencies to identify privacy challenges on an IT system analysing Data protection regulations, GDPR, NIST and other which are relevant for enterprises and organisations
- Must have competencies to apply privacy theories and data protection to a specific system or technology
- Must have competencies to apply ethical criteria to privacy and data protection to provide a more diverse understanding these and what they mean

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Data Protection and Privacy
Type of exam	Written or oral exam
ECTS	5

Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Databeskyttelse og privacy
Module code	ESNMCSPM1K2
Module type	Course
Duration	1 semester
Semester	Autumn
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Education owner	Master of Cyber Security and Privacy
Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	The Technical Faculty of IT and Design

COMPLIANCE AND THE ENTERPRISE

2023/2024

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

The aim of this project is to analyse the compliance of different technologies in the enterprise and assess its impact on the enterprise business and present overview of technologies, its cyber security challenges individually and as an IT system landscape of the common enterprise/organizational technologies.

LEARNING OBJECTIVES

KNOWLEDGE

- Must have knowledge about enterprise security standards
- Must have knowledge about enterprise security architectures
- Must have knowledge about emerging technologies relevant for enterprises and their security and privacy aspects

SKILLS

- Must be able to discuss the role of security standards on governance of security in a specific enterprise
- Must have the ability to perform risk assessment and come up with mitigation strategies
- Must be able to develop secure solutions based on emerging technologies
- Must be able to assess, compare and select technologies to secure existing systems

COMPETENCES

- Must have the competencies to develop compliant IT and security strategies for an enterprise
- Must have the competencies to develop compliant privacy data-protection strategies for an enterprise
- Must have competencies to select a case form a specific enterprise, perfume security analysis and assess which security standards, architectures and technologies to be used to mitigate the vulnerability
- Must have the competencies to assess the role of emerging technologies to create secure solutions for enterprises

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Compliance and the Enterprise
Type of exam	Oral exam based on a project
ECTS	10
Assessment	7-point grading scale
Type of grading	External examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Compliance og entreprisen

Module code	ESNMCSPM2P1
Module type	Project
Duration	1 semester
Semester	Spring
ECTS	10
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Education owner	Master of Cyber Security and Privacy
Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	The Technical Faculty of IT and Design

ENTERPRISE SECURITY AND COMPLIANCE

2023/2024

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

The purpose of this course is to understand cyber security challenges, technologies and the policies and standards enterprises need for compliance. Security and compliance are discussed with respect to enterprise technologies. The course is tightly correlated with the course in Enterprise technologies.

LEARNING OBJECTIVES

KNOWLEDGE

Must have knowledge of:

- standards addressing information security and cyber security challenges
- technologies already embedded in enterprise endpoints
- security services and policies within public and private cloud networks

SKILLS

Must be able to:

- identify and manage risks in combination with security requirements
- design, implement and verify enterprise security solutions
- identify and illustrate an IT system landscape end-to-end and pinpoint risks to be considered
- carry out an information security review and an IT audit

COMPETENCES

Must have the competency to:

- design requirements and controls for an enterprise security solution based on a risk assessment
- discuss end-to-end standards to create trust and controls in a large enterprise IT solution.
- discuss the business needs and willingness to accept risks based on an Enterprise Risk Management solution
- discuss risks, security and compliance in a cloud environment.

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Enterprise Security and Compliance
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Enterprise sikkerhed og compliance
Module code	ESNMCSPM2K1
Module type	Course
Duration	1 semester
Semester	Spring
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Education owner	Master of Cyber Security and Privacy
Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	The Technical Faculty of IT and Design

EMERGING TECHNOLOGIES AND SECURITY

2023/2024

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

The purpose of this course is to introduce central current and future technologies, which are central to enterprises and organizations. Understanding technologies, concepts and purpose will contribute to a better understanding of cyber security and privacy related to these. The enterprise systems and technologies include, AI, cloud, blockchain, large enterprise systems and others.

LEARNING OBJECTIVES

KNOWLEDGE

- Must have knowledge about IoT devices and the usage of cloud computing in complex IoT architectures.
- Must have knowledge about privacy and security considerations of such architectures.
- Must have knowledge about different virtualization techniques, how they are used to support the cloud and their security characteristics.
- Must have knowledge about AI and its use in detection of security and privacy vulnerabilities in large enterprise systems
- Must have knowledge about Blockchain and its use in distributed organisations

SKILLS

- Must be able to design and implement secure solutions for enterprises that make use of IoT devices and the cloud.
- Must be able to use common frameworks for developing secure IoT solutions provided by the biggest cloud providers.
- Must be able to assess when and where to use AI or Block Chain to solve privacy and security tasks in organisational systems

COMPETENCES

- Must have competencies to design and implement secure solutions based on one or more of emerging technologies thought in the course.

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Emerging Technologies and Security
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Fremspirende teknologier og sikkerhed
Module code	ESNMCSPM2K2
Module type	Course
Duration	1 semester
Semester	Spring
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Education owner	Master of Cyber Security and Privacy
Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	The Technical Faculty of IT and Design

MASTER'S PROJECT: STRATEGIES FOR SECURE ORGANISATIONS

2023/2024

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

The aim of this project is to carry out security risk and threat analysis of a chosen technology, system or enterprise/organization and asses or implement mitigation strategies for dealing with these. Students can base the security analysis on actual testing of system (using for example penetration testing or the like) or create an analytical end-to-end description of the threats and risks. The analysis shall be used as a basis for creating a strategy for diminishing the threats and risks

LEARNING OBJECTIVES

KNOWLEDGE

- Must have knowledge of different cyber treats, including threat actors and attack vectors.
- Must have knowledge of relevant methods and frameworks for risk assessment, including ISO27001/ISO27002 and NIST.
- Must have knowledge of relevant frameworks for understanding cyber-attacks, including the Cyber Kill Chain as well as the Mitre att&ck framework.

SKILLS

- Must have the ability to choose and describe relevant mitigation strategies, based on a cyber risk analysis.
- Must have the ability to select and apply methods and techniques to find known vulnerabilities in systems, i.e. using penetration-testing tools as well as OSINT techniques.
- Must have the ability to develop incident response plans along with procedures for testing and revising such plans.

COMPETENCES

- Must have competences in choosing and applying relevant methods and framework to conduct cyber risk analysis for a system.
- Must have competences in critically reflecting on the limitations, strengths and drawbacks of the selected methods.
- Must have competences in developing a strategy to mitigate and handle cyber risks, based on the analysis carried out with respect to a system.
- Must have competences in presenting the conducted assessments to a broad audience within an organisation.

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Master's Project: Strategies for Secure Organisations
Type of exam	Master's thesis/final project
ECTS	15
Assessment	7-point grading scale
Type of grading	Internal examination

Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Masterprojekt: Strategier for sikker organisationer
Module code	ESNMCSPM3P1
Module type	Project
Duration	1 semester
Semester	Autumn
ECTS	15
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Education owner	Master of Cyber Security and Privacy
Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	The Technical Faculty of IT and Design

MASTER'S PROJECT: PRIVACY AND DATA PROTECTION STRATEGIES

2023/2024

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

The aim of this project is to focus on privacy and carry out privacy and data protection analysis of a chosen technology, system or enterprise/organization and discuss mitigation strategies for dealing with these. Students must base their analysis on privacy theories and data flow diagrams and base this as the foundation for developing strategies to deal with this.

LEARNING OBJECTIVES

KNOWLEDGE

- Must have knowledge about methods for understanding privacy data risk
- Must have knowledge about methods for representing data spread in and out of an enterprise system
- Must have knowledge about theories for understanding human introduced risks relating to data protection and privacy
- Must have knowledge about central concepts relating to privacy and data protection, such as GDPR, privacy definitions etc.

SKILLS

- Must have the ability to make an analysis of a selected enterprise with respect to privacy and data protection
- Must have the ability to carry out a risk analysis of a selected enterprise with respect to data protection and privacy
- Must have the ability to use central methods such as data flow diagrams, and others to visualise data spread and provide a scalable understanding of the privacy and data protection risks
- Must have the ability to describe an enterprise system and its data protection and privacy elements, implemented and challenges

COMPETENCES

- Must have competencies in presenting an overview of privacy and data protection challenges for a selected enterprise system
- Must have competencies in using established knowledge about privacy and data protection to create strategies for improvement or even for mitigation of the privacy the data protection challenges
- Must have competencies for presenting results of the work for an enterprise to provide feedback and knowledge to the enterprise for the work

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Master's Project: Privacy and Data Protection Strategies
Type of exam	Master's thesis/final project
ECTS	15
Assessment	7-point grading scale

Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Masterprojekt: Privacy og databeskyttelse strategier
Module code	ESNMCSPM3P2
Module type	Project
Duration	1 semester
Semester	Autumn
ECTS	15
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Education owner	Master of Cyber Security and Privacy
Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	The Technical Faculty of IT and Design

MASTER'S PROJECT: GOVERNANCE OF SECURITY 2023/2024

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

The topic of this project is the relationships between technical, economic- political-, regulatory and cultural aspects of cyber security threats for individuals, companies, organizations and nations. The aim is that the students must understand the interplay between these aspects of cyber security and how precautions require solutions that include technical as well as political-regulatory and normative initiatives. Furthermore, the students must be able to operationalize knowledge on complex cyber security problems in managerial initiatives at strategic and tactical levels.

LEARNING OBJECTIVES

KNOWLEDGE

Must have knowledge:

- on problems within cyber security, that individuals, companies, organizations, public institutions and nations can encounter
- on the interrelationships between technical, economic, political-regulatory and cultural aspects of threats against cyber security
- on how the interplay between technical, political-regulatory and normative precautions can limit threats against cyber security
- on legal requirements, standards and certification arrangements concerning cyber security at national and EU level respectively
- on strategic and tactical management of cyber security within organizations, including norms for strengthening of the protection of personal data and cyber security
- about the relation between security risks and business processes including the identification and protection of business-critical assets

SKILLS

Must have skills:

- in detecting new risks and threats concerning cyber security within companies and other organizations
- in being able to contribute to the development of methods to protect cyber security
- in management of the prevention and control of threats against cyber security
- in developing security strategies that include technical as well as normative aspects

COMPETENCES

Must have competences:

- to reflect on the ethical issues which the processing of sensitive personal data can involve
- in understanding complex security problems
- in communicating cyber security challenges and solutions to non-experts

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Master's Project: Governance of Security

Type of exam	Master's thesis/final project
ECTS	15
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Masterprojekt: Styring af sikkerhed
Module code	ESNMCSPM3P3
Module type	Project
Duration	1 semester
Semester	Autumn
ECTS	15
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Education owner	Master of Cyber Security and Privacy
Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	The Technical Faculty of IT and Design

USABLE PRIVACY AND SECURITY

2023/2024

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

Technology in itself cannot secure that enterprises, organisations and systems are secure. Humans are essentially responsible for the majority of privacy and security breaches, and therefore they play an important role in understanding how levels of privacy and security can be improved. This course focuses on understanding the interplay between humans and enterprise systems, as well as identifying ways to improve this for the greater sense of the enterprise security and privacy.

LEARNING OBJECTIVES

KNOWLEDGE

- Must have knowledge about user security and how it links to how users behave
- Must have knowledge about the term “social engineering”
- Must have knowledge about data flow diagrams to understand data spreading
- Must have knowledge about theories for how users interact with systems and what impact that can have on security and privacy
- Must have knowledge about methods for understanding how users interact with enterprise systems
- Must have knowledge about different strategies for how to impact on user behaviour in order to increase privacy and security

SKILLS

- Must have the ability to use theories that are reflecting how users behave with enterprise systems
- Must have the ability to work with users in order to understand what and how privacy and security elements in an enterprise system are perceived and handled
- Must have the ability to identify discrepancies in systems interface design with respect to privacy and security
- Must have the ability to link the user security and privacy to system set-ups and how interfaces are built
- Must have the ability to use “social engineering” on existing organisational/business enterprise web-sites to understand the risks of privacy and security

COMPETENCES

- Must have competencies in using theories of user interaction and user behaviour on selected enterprice systems
- Must have competencies in designing solutions which can address security and privacy discrepancies in systems interface design and user behaviour
- Must have competencies in redesigning unfortunate interfaces which are connected with a security or privacy risk.

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Usable Privacy and Security
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale

Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Usable privacy og sikkerhed
Module code	ESNMCSPM3K1
Module type	Course
Duration	1 semester
Semester	Autumn
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Education owner	Master of Cyber Security and Privacy
Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	The Technical Faculty of IT and Design

ADVANCED NETWORK AND SYSTEM SECURITY

2023/2024

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

In this course, the students learn to protect networks and systems against cyber attacks, and they learn to analyse and test network/system for vulnerabilities. Such systems can be based either on software alone, or it can be cyber physical systems consisting of both hardware and software elements. It can also be an embedded system, or a distributed system connected through one or more networks. The course includes advanced topics in network security, including intrusion detection/prevention, deception technologies, and the underlying theories and methods.

LEARNING OBJECTIVES

KNOWLEDGE

- Must have knowledge of methods and techniques for monitoring networks and systems in order to prevent and detect cyber-attacks, including intrusion detection and intrusion prevention systems.
- Must have knowledge of deception technologies, such as different kinds of honeypots and their limitations.
- Must have knowledge of covert channels and steganography.

SKILLS

- Must have skills in analysis and testing of systems and networks in order to uncover relevant cyber risks and attack vectors, including network scanning and penetration testing.
- Must have skills in prevention of cyber-attacks in networks and systems by selecting and establishing relevant countermeasures.
- Must have skills in gathering network traffic and network traffic data.
- Must have skills in configuration and operation of secure test environments

COMPETENCES

- Must have competences in assessing, selecting and applying methods in order to secure and/or to conduct security testing of a given system, evaluate the specific results generated by using these methods, as well as reflecting over approach and results
- Must have competences in understanding Internet-based threats and attack techniques, including DoS (Denial of Service) attacks, DDOS (Distributed Denial of Service) attacks, exploitation of vulnerabilities, lateral movement, and information theft.
- Must have competences in fundamental techniques within network traffic monitoring, including active and passive monitoring techniques and the application within detection of malicious network activities

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Advanced Network and System Security
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale
Type of grading	Internal examination

Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Avanceret netværks- og systemsikkerhed
Module code	ESNMCSPM3K2
Module type	Course
Duration	1 semester
Semester	Autumn
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Education owner	Master of Cyber Security and Privacy
Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	The Technical Faculty of IT and Design

REGULATION OF CYBER SECURITY

2023/2024

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

The aim of the course is to provide the students with an overview of the legal and institutional framework conditions for cyber security and how they are applied. The course includes relevant national and international legislation and regulation within the area including EU directives and regulations. Focus is on cybercrime, privacy, logging, and problems within digital media, the financial sector and national security.

LEARNING OBJECTIVES

KNOWLEDGE

- Must have knowledge on the various kinds of legislation and regulation
- Must have specific knowledge on legislation concerning cyber security in Denmark and the EU
- Must have knowledge on legislation and regulation regarding digital media
- Must have knowledge on the most important organizations within the development of standards and certification regarding cyber security and digital signature

SKILLS

- Must have skills with respect to detecting problems in cyber security in the financial sector
- Must have skills in correctly handling sensitive data including personal data taking current legislation into account
- Must have skills in being able to identify security requirements and solutions with implications for national security
- Must have skills in being able to include techno-economic considerations in an analysis of technical and organizational solutions in cyber security

COMPETENCES

- Must have competences to assess technical solutions in cyber security in light of the specific organizational conditions and legal frameworks
- Must have competences to include ethical issues in relation to the analysis of a concrete security solution

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Regulation of Cyber Security
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Regulering af cybersikkerhed
Module code	ESNMCSPM3K3
Module type	Course
Duration	1 semester
Semester	Autumn
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Education owner	Master of Cyber Security and Privacy
Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	The Technical Faculty of IT and Design