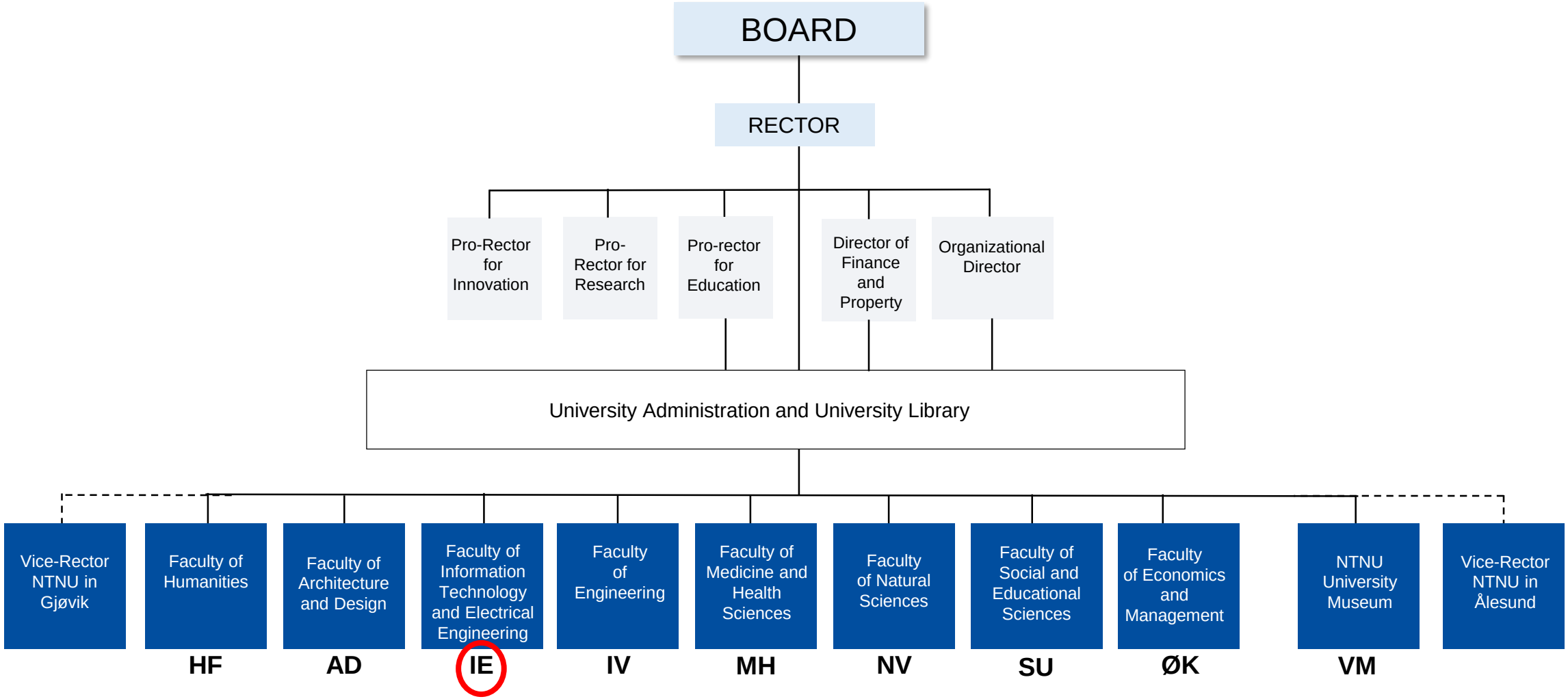
NTNU Organization



Faculty of Information Technology and Electrical Engineering (IE)

- Department of General Science
- Department of Computer Science
- Department of Electronic Systems
- Department of Electric Power Engineering
- Department of ICT and Natural Sciences
- Department of Information Security and Communication Technology
- Department of Mathematical Sciences
- Department of Engineering Cybernetics

Department of Information Security and Communication Technology

- Two campuses
  - Trondheim
  - Gjøvik
- The Department conducts international competitive research in several areas of cyber security, information security, communication networks and networked services.
- The department operates study programs in information security and communication technology at Ph.D, M.Sc. and B.Sc. levels.
- It also hosts Center for Cyber and Information Security (CCIS) and the national Research School of Computer and Information Security (COINS).

Department of Information Security and Communication Technology

- Bachelor programmes
  - 3-year BSc in IT Operations and Information Security
- Master programmes
  - 5-year MSc in Communication Technology (in Norwegian only)
  - 2-year MSc in Communication Technology
  - 2-year MSc in Information Security
  - 2-year Master Programme in Security and Cloud Computing (SECCLO)
  - 1.5-årig Experience Based Master's in Information Security
- PhD programmes

Master Programme in Security and Cloud Computing (SECCLO) at NTNU

- Second year specialization at NTNU: Information Security
- There are 3 mandatory courses and one elective course from a set of 6 courses
- The students learn about authentication, key distribution, integrity, confidentiality, anonymity and digital forensics in wireless access networks for mobile users, as well as proposed new network technologies. A course on ethical hacking covers techniques used by computer hackers and penetration testers in order to better defend against intrusions and security violations in live systems, including low-level kernel and hardware topics, techniques for web applications, exploit techniques, rootkits, and some forensic techniques.
- The students perform a small research project and learn the phases of research from motivation to evaluation of the results. The project prepares the students for the thesis.

Master Programme in Security and Cloud Computing (SECCLO) at NTNU

- Mandatory courses (22.5 ECTS):
  - Wireless Network Security (7.5 ECTS)
  - Ethical Hacking – Information Security (7.5 ECTS)
  - Telematics, Specialization Project (7.5 ECTS)

Master Programme in Security and Cloud Computing (SECCLO) at NTNU

- **Wireless Network Security (7.5 ECTS)**
  - The course presents security techniques employed in existing systems, such as WPAN, WLAN, UMTS, IMS. Proposed solutions for new network technology, such as various types of ad-hoc networks.
- Learning outcome
  - **A. Knowledge:** of methods for communication systems that provide services for mobile users by wireless access networks. Understanding of security mechanisms and protocols in wireless communication systems, such as the topical technologies of WLAN IEEE 802.11, WAN 802.16, GSM/UMTS/LTE, Ad-hoc and sensor networks. Models, design principles, mechanisms and solutions used in wireless network security to obtain authentication and key transport protocols.
  - **B. Skills:** 1. analytical skills in information security assessment of technology and methods for communication systems that provide services for mobile users by wireless access networks; 2. collaboration work (ideally three students) that perform a week of lab project problem solving of WLAN security analysis and construction, including keeping a lab journal and writing up a lab report afterwards. 3. Each student selects after interests and motivation, under supervision, a technical topic to study within wireless security that is not part of the lectured syllabus, and writes a short concise technical essay (~4 pages) presenting the topic studied.

Master Programme in Security and Cloud Computing (SECCLO) at NTNU

- **Ethical Hacking – Information Security (7.5 ECTS)**
  - The course covers the main techniques used by computer hackers and penetration testers in order to better defend against intrusions and security violations in live systems, including low-level kernel and hardware topics, techniques for web applications, exploit techniques, rootkits and some audit techniques used in digital forensics.
- Learning outcome
  - **A. Knowledge:** Students will learn the underlying principles and techniques associated with the cybersecurity practice known as penetration testing or ethical hacking. They will become familiar with the entire penetration testing process including planning, reconnaissance, scanning, exploitation, post-exploitation and result reporting.
  - **B. Skills:** For every offensive penetration technique the students will learn the corresponding remedial technique. By this, the students will develop a practical understanding of the current cybersecurity issues and the ways how the errors made by users, administrators, or programmers can lead to exploitable insecurities.
- Learning methods and activities
  - Lectures, seminars, invited lectures, student presentations and laboratory exercises. Two compulsory practical ethical hacking tasks; both tasks must be approved to qualify for the final exam.

Master Programme in Security and Cloud Computing (SECCLO) at NTNU

- **Telematics, Specialization Project (7.5 ECTS)**
  - Preparatory project for the master's thesis.
  - Choose a research assignment, optionally an advanced development task with research elements.
  - Address the problem by, i.a., studying background literature in the field, current research literature and, if relevant, through discussions with the "problem owner".
  - Give a motivation for the assignment.
  - Describe the state of the art / research front in the field.
  - Formulate specific objective(s) / research question(s) / hypothesis (s) for the master's thesis.
  - Establish and describe a proposed method to achieve the objective(s) and, if relevant, verify the result.
  - Familiarise with and test the tools that are planned to be used in the work.
  - Prepare an initial plan for the work towards the master's thesis, i.e., a division into tasks, progress, resource utilisation and milestones.
  - As far as the time permits, the candidate should conduct and report preparatory work on the assignment.

Master Programme in Security and Cloud Computing (SECCLO) at NTNU

- Elective courses (7.5 ECTS):
  - Enterprise Architecture for Enterprise Innovation (7.5 ECTS)
  - Introduction to Digital Forensics (7.5 ECTS)
  - Introduction to Information Security Management (7.5 ECTS)
  - Critical Infrastructure Security (7.5 ECTS)
  - Intrusion Detection in Physical and Virtual Networks (7.5 ECTS)
  - Introduction to Data Privacy (7.5 ECTS)

Master Programme in Security and Cloud Computing (SECCLO) at NTNU

- **Enterprise Architecture for Enterprise Innovation (7.5 ECTS)**
  - This course focuses on the role of information systems in an organizational context, both used internally in organizations and to support the organization's involvement in collaboration e.g. through digital ecosystems. Emphasis is placed on how IT can support innovation and new services design and bring value to an organization. The course will address methods for business modeling, service design and enterprise modeling that are complementary to systems modeling. Methods related to modeling and quality assurance of models will be presented. Enterprise Architecture methods will also be presented.
- Learning outcome
  - **A. Knowledge:** The candidate shall establish theoretical insights into business and enterprise modeling, service innovation and the methods for analysing organizational situations and modeling them.
  - **B. Skills:** The candidate shall establish practical skills in creating good business and enterprise models that enhances the understanding of the design of IT systems and the perspectives of software engineering models.
- Learning methods and activities
  - Lectures, term paper and exercises.

Master Programme in Security and Cloud Computing (SECCLO) at NTNU

- **Introduction to Digital Forensics (7.5 ECTS)**
  - Digital investigations, stakeholders and their roles; Digital evidence, e.g. acquisition, admissibility, authenticity; Chain of custody, evidence integrity and forensic soundness; File and live system forensics; Timeline analysis; Forensic reconstructions; Internet and network forensics; Automation and forensic tools; Reporting and presenting evidence; Expert witness and cyber crime law; Computational forensics; Forensic readiness; Advanced topics
- Learning outcome
  - **A. Knowledge:** Understanding of requirements for handling digital evidence; Requirements and impact on maintaining evidence integrity and chain of custody; Principles, procedures, and the basic concepts of forensic standards and best practices, e.g. forensic tool testing; The overall process for establishment and maintenance of a digital forensic lab environment; The role of expert witnesses and digital evidence in the context of legal proceedings; The role of policies, standards and guidelines for controls and is capable of applying his/her knowledge in case studies; Legal, privacy and ethical aspects of digital forensics investigations.
  - **B. Skills:** Forensic acquisition of digital evidence from computer and network media; Live system forensics and evaluation of order of volatility; Evidence analysis with timeline analysis and forensic reconstruction; Scientific documentation of forensic acquisition and analysis; Applying forensic principles on practical case-studies; Performing stakeholder analysis, risk assessment and forensic triage on limited case-studies; Evaluating the applicability of forensic methods and tools for various controls given a certain scope and policy for the control
- Learning methods and activities
  - Lectures, Group work, Lab work, E-learning, Project work

Master Programme in Security and Cloud Computing (SECCLO) at NTNU

- **Introduction to Information Security Management (7.5 ECTS)**
  - Introduction to System Thinking and Scientific Management; Cultural, Organization and Behavior theories used information security management organization; Legal and Ethical Aspects of Information and Privacy Management; Overview of current information security management standards and practices; Basic Micro and Macro Theory of Information Security; Introduction to Risk, Threat and vulnerability Modeling; Information Security Management and Security Awareness education and training; Overview of Security Planning and Incident Management
- Learning outcome
  - **A. Knowledge:** of the fundamental theories, models practices of information security management for both large and small organizations; understanding of ethical and legal aspect of information security management and privacy management; of the risk management processes; of security planning and incident management process; of security awareness and security escalations issues in information security management work; of both macro and micro economics issues in information security management; of the technological innovation process in IT security and its effect on security management; of the standards in information security management
  - **B. Skills:** capable of analyzing existing theories, models and methods in the field of information security management and work independently on solving theatrical and practical problems; capable of applying his/her knowledge to both modeling the potential problems and the solutions in information security management and be able to communicate this problems and solutions using basic rhetorical skills; capable of using and the basic terminology and is aware of the basic standards used in the area.
- Learning methods and activities
  - Lectures, Group work, E-learning, Assignments, Project work, Reflection, Seminar(s)

Master Programme in Security and Cloud Computing (SECCLO) at NTNU

- **Critical Infrastructure Security (7.5 ECTS)**
  - Critical Infrastructures and Information Infrastructures; Threat Actors and Agents in Critical Infrastructures; Infrastructure Modeling, Robustness, and Dependencies; Cyber-Physical Systems and their Security; -Control Systems Security; Selected Aspects of Critical Telecommunications Infrastructure Security and Resilience; Selected Aspects of Power Networks and Generation Infrastructure Security and Resilience; Selected Aspects of Oil and Gas Infrastructure Security and Resilience; Selected Aspects of Transportation Infrastructure Security and Resilience
- Learning outcome
  - **A. Knowledge:** of core concepts of critical information infrastructures and general critical infrastructure as well as their dependencies; of infrastructure and infrastructure robustness models; of cyber-physical systems and control systems security.
  - **B. Skills:** to analyze threat modeling approaches and to assess their suitability for a given set of threat sources and agents; to critically analyze existing theories and methods for the study of cyber-physical systems security and to independently apply such methods to related problems; to carry out research in selected areas of infrastructure security and resilience under guidance and supervision; to identify and critically analyze primary research literature on critical infrastructure security and to apply appropriate scientific reasoning
- Learning methods and activities
  - Lectures, Group work, E-learning, Assignments, Project work, Reflection, Seminar(s)

Master Programme in Security and Cloud Computing (SECCLO) at NTNU

- **Intrusion Detection in Physical and Virtual Networks (7.5 ECTS)**
  - IDS/IPS definition and classification; Basic elements of attacks and their detection; Misuse detection systems (search algorithms and applications in IDS); Anomaly detection systems (machine learning basics: principles, measures, performance evaluation, method combinations, basics of artificial neural networks, clustering (hierarchical and partitional) and supervised learning in IDS); Testing IDS and measuring their performances; Computational complexity-theoretic and information-theoretic IDS models and quality criteria; Intrusion detection in virtual networks.
- Learning outcome
  - **A. Knowledge:** in detection/prevention of intrusions in computer systems and networks, in application of advanced search algorithms in intrusion detection, unsupervised and supervised learning methods used in these systems, computational complexity-theoretic modeling, information-theoretic modeling of intrusion detection/prevention systems, and intrusion detection in virtual networks; knowledge about theory and scientific methods relevant for intrusion detection.
  - **B. Skills:** capable of analyzing existing theories, methods and interpretations in the field of intrusion detection and working independently on solving theoretical and practical problems; to use relevant scientific methods in independent research and development in intrusion detection; 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; capable of carrying out an independent limited research or development project in intrusion detection under supervision, following the applicable ethical rules.
- Learning methods and activities
  - Lectures, Lab work, Assignments

Master Programme in Security and Cloud Computing (SECCLO) at NTNU

- **Introduction to Data Privacy (7.5 ECTS)**
  - This course is centered on theory and methods for statistical disclosure control, formal definitions of privacy in databases containing population data, syntactic and differential privacy and their respective suitability for balancing privacy costs with information benefits, mechanisms for creating differentially private algorithms for querying data. In addition it discusses ethical and political foundations for why privacy is needed and frame privacy in terms of a tradeoff between individual privacy and societal benefit.
- Learning outcome
  - **A. Knowledge:** good understanding of aspects of data privacy, ranging from the philosophical, through the political and organizational, to the technical. She will know privacy as a process of adapting to a changing circumstance. The student will also know the significance of randomness in protecting privacy and quantifying risk, and be able to operationalize this understanding.
  - **B. Skills:** to identify privacy related aspects of data uses; to identify relevant regulatory requirements of data uses; to apply differentially private mechanisms when statistic or utility sensitivity to changes in data is readily available.
- Learning methods and activities
  - Lectures, Lab work, Assignments, Exercises.

Thank you