ACADEMIC REGULATIONS

Master's degree programme

in

CYBERSECURITY ENGINEERING

Department of Control and Computer Engineering

Collegio di Ingegneria Informatica, del Cinema e Meccatronica

Academic Year **2025/2026**

The English translation of this document is provided as a support to the student community and has no legal effects. The Italian version shall constitute the sole authentic text and will be referred to for any legal matters.

SUMMARY

Art. 1 – Specific learning objectives and career prospects

1.1 Specific learning objectives

In today's world, cyber-physical systems have become a pervasive and essential component of modern society, playing an ever-growing role in daily activities. The devices and environments in use are increasingly intelligent, interconnected, dynamic, and flexible. At the same time, cyber threats are growing rapidly, along with the regulations and standards that every company, organization, or country must comply with in order to avoid being vulnerable to attacks and to other cyber-related risks.

In this context, cybersecurity professionals must have a highly specialized and comprehensive knowledge background. In addition to a solid scientific and technological foundation, cybersecurity experts are expected to have legal competencies in both civil law (e.g., managing European privacy regulations such as the GDPR) and criminal law (e.g., conducting forensic analyses), as well as knowledge in business and management (e.g., managing cyber risk in an economically informed way).
The decision to establish a new Master's degree programme arises from the need to integrate interdisciplinary legal and economic skills with a robust technological background in computer engineering, encompassing software, hardware, and computer networks. The aim is to train professionals with a high level of expertise in cybersecurity.

The Master's degree programme in Cybersecurity Engineering is a multi-class programme, fulfilling the educational objectives of both the Master's degree class in Computer Engineering (LM-32) and the degree class in Cybersecurity (LM-66 R).

The Master's degree programme in Cybersecurity Engineering fully reflects the educational objectives of the degree class in Cybersecurity (LM-66 R), through core learning activities in the following areas:

- Scientific: with in-depth study of modern cryptography and the emerging challenges brought by quantum computing
- Technological and IT-related: by providing advanced knowledge of the methodologies and technological tools used to design, implement, verify, and maintain secure and protected IT infrastructures and systems
- Legal, social, and economic: essential to apply and comply with national, European, and international laws and regulations on privacy and data protection in the context of cybersecurity, as well as to understand cybersecurity management models and define effective corporate strategies.

At the same time, for professional who need to manage the security of complex IT systems, it is crucial to acquire advanced technological knowledge in the field of computer engineering—core to the educational objectives of the LM-32 degree class—particularly in the following areas:

- computer networks, cloud systems, and web infrastructures
- computer architectures and embedded/IoT systems
- wireless, Bluetooth, and cellular communication systems
- software systems and the various programming techniques.

1.2 Career prospects

The Master's degree programme aims to train a variety of professional profiles. The career prospects and the main functions and competencies associated to each profile are illustrated below.

Professional profile	Main functions and competencies
Cyber Analyst	Functions: Cyber Analysts are specialists who run and assess the exposure to cyber risks and the corresponding mitigation strategies. They monitor and evaluate the effectiveness of an organization's security posture, identify system vulnerabilities and possible ways to exploit them, ensure business continuity and service recovery, investigate the causes and motivations of cyberattacks, and conduct digital crime investigations. Competencies: Cybersecurity Analysts adopt a comprehensive approach to assessing an organization's exposure to cyber threats. They can: • manage cyberattacks and incidents, oversee the activities of a Security Operations Centre (SOC), and operate within a Computer Security Incident Response Team (CSIRT); • master the main methodologies and tools for planning, designing, and conducting vulnerability assessments and penetration testing; • simulate software and hardware attacks to evaluate the effectiveness of security measures; • apply and leverage digital forensics methods, tools, and practices to investigate the origin and nature of cybercrimes. Potential Employers: Cyber Analysts are in demand at medium and large enterprises, software and hardware development companies, public administrations, national defence and security agencies, and public or private offices tasked with investigating cybercrime.
Cyber Designer	Functions: Cyber Designers are specialists who work on the design, review, and improvement of cybersecurity aspects within systems. They contribute to the development, implementation, and maintenance of security solutions, with responsibilities ranging from the actual design of secure systems to the coordination, integration and ongoing management of security measures. Competencies: Cyber Designers can design key security solutions for information systems based on risk assessments, regulatory standards, and applicable legal frameworks. They identify and assess risk factors and potential threats to infrastructures, comparing them against reference models, paradigms, architectures, and security technologies. They can develop, deploy, manage, and maintain cybersecurity solutions (including systems, resources, software, controls, and services) across infrastructures and products. Potential Employers: Cyber Designers are mainly employed by large companies, consulting firms, software and hardware development companies, public administrations, and national security agencies. They are also sought after by small and medium-sized enterprises that want to reduce their exposure to cyber risks.
Cryptography Expert	Functions: Cryptography Experts specialize in techniques, mechanisms and development of tools to ensure data and communication integrity and confidentiality. They evaluate, design and develop both basic and advanced cryptographic applications and systems. Competencies: They analyse and develop cryptographic and communication protocols, including protocols related to advanced technologies and topics such as Post-Quantum Cryptography, Blockchain and its applications, Cryptocurrencies and Tokens, Functional and Homomorphic Encryption, Cryptanalysis, and Zero-Knowledge Proofs. Potential Employers: Cryptography Experts are primarily employed by medium and large enterprises, consulting firms, companies developing or producing cybersecurity products, and national security and defence agencies.
Cyber Legal and Compliance Officer	Functions: Cyber Legal and Compliance Officers manage and assess the compliance of digital systems and ecosystems with national, European, and international laws and regulations on data protection and cybersecurity. They ensure that adopted security strategies and solutions meet legal requirements,

	reference standards, and corporate contracts. Specifically, they: • ensure compliance and provide legal advice on privacy, data protection, and applicable laws and regulations; • ensure that data controllers, processors, internal stakeholders, partners, and third parties are informed of their rights, duties, and responsibilities under data protection laws; • are the key liaison between technical and legal/commercial departments • support the design, implementation, verification, and testing of compliance with cybersecurity standards and laws; • conduct or coordinate audits and training activities related to data protection and corporate security. Competencies: Cyber Legal and Compliance Officers can assess whether adopted security strategies and solutions comply with legal requirements, standards, or contractual obligations. They carry out the tasks listed above in close cooperation with both technical and legal teams. Potential Employers: Cyber Legal and Compliance Officers are employed by public administrations, private organizations, consulting firms, and companies of all sizes developing cybersecurity solutions.

1.3 Professional profiles (ISTAT codes)

With reference to the list of professional profiles classified by ISTAT (Italian National Institute of Statistics, https://www.istat.it/en/), graduates from this Master's degree programme can work as:

ISTAT code	Description
2.1.1.4.2	Analisti di sistema
2.1.1.4.3	Analisti e progettisti di applicazioni web
2.1.1.5.1	Specialisti in reti e comunicazioni informatiche
2.1.1.5.4	Specialisti in sicurezza informatica

Art. 2 – Admission requirements

Italian regulations on enrolment in Master's degree programmes require Italian universities to check that applicants meet the following requirements:

- have a **three-year Bachelor's degree or university diploma**, or **other educational qualification obtained outside Italy** and recognized as suitable for admission;
- meet specific curricular requirements;
- have an **academic performance considered suitable** for admission.

CURRICULAR REQUIREMENTS

As far as curricular requirements are concerned, applicants must have a Bachelor's degree belonging to one of the following classes: Ingegneria dell'Informazione (L-8) o in Scienze e Tecnologie informatiche (L-31) or an educational qualification obtained outside Italy and recognized as suitable for admission.

Alternatively, applicants must have earned:

- at least 40 credits in the following Scientific Disciplinary Fields (settori scientifico-disciplinari): FIS/01, FIS/03, INF/01, ING-INF/05, MAT/02, MAT/03, MAT/05

and

- at least 60 credits earned in the following Scientific Disciplinary Fields (settori scientifico-disciplinari): INF/01, ING-INF/01, ING- INF/03, ING-INF/05, SECS-S/01, MAT/03, MAT/05, MAT/06, MAT/08, MAT/09.

The curricular requirements are automatically met by the applicants who have a Bachelor's degree belonging to classes L-8 o L-31. In all other cases, admission applications will be evaluated by the Academic Advisor of the degree programme, or by a delegate, who will decide and motivate the credit equivalence for the Scientific Disciplinary Fields that are different from the ones established by the present Regulations.

The credits of the Scientific Disciplinary Fields found both in the first group and in the second group are primarily counted for the first group. The remaining credits are counted for the second group. Therefore, the credits of a course can be counted partly to reach the minimum number of credits of both groups.

Applicants who lack less than 10 credits may be admitted to the programme by the Academic Advisor. For applicants who lack more than 10 credits, the evaluation will be subject to the final approval of the Coordinator or the Vice coordinator of the degree programme.

Applicants who do not meet the curricular requirements are required to make up for their unfulfilled curricular requirements (missing credits) before enrolment, by means of:

- **enrolment in single courses in order to make up for unfulfilled curricular requirements**: this is possible for students who need to earn up to a maximum of 60 credits. Students who enrol in single courses for this reason are allowed to include in their Personal Study Plan exclusively the courses assigned by the evaluator.
  or else,
- **credit transfer at Bachelor's level:** this is possible for students who need to earn more than 60 credits. In this case, students need to enrol in the Bachelor's degree programme that offers the credits in the specific Scientific Disciplinary Fields (core subjects and commentary subjects) required for admission to this Master's degree programme.

SUITABLE ACADEMIC PERFORMANCE

Applicants must have a suitable academic performance and an English language certificate (B2 level or above, as defined by the Common European Framework of Reference for Languages: Learning, Teaching, Assessment - CEFR).

The academic performance will be assessed as follows.

1) Applicants from Politecnico di Torino

Applicants can be admitted to the programme if they earned their Bachelor's degree in:

- 4 years (1) or less - no exam average grade required
- between 4 and 5 years (1) –exam weighted average grade required (2): ≥21/30

- more than 5 years– exam weighted average grade required (2): ≥ 24/30

The weighted average grade is calculated on all accrued course credits (graded on a scale of 30) counting towards the achievement of the Bachelor's degree, after having subtracted the worst 28 credits.

The duration of the Bachelor's path is calculated on the basis of the number of academic years in which the applicant has been enrolled at the university, starting from the first enrolment in the Italian university system:

- for full-time students: the duration of the Bachelor's path is equivalent to the number of academic years of enrolment.
- for part-time students: each year of enrolment is counted as half-year.
- for full-time students taking part in the "Dual Career" programme: each year of enrolment is counted as half-year, as for part-time students.

In the event of credit transfer, the duration of the Bachelor's path must be increased proportionally to the number of credits that have been recognized by Politecnico (10-60 CFU =1 year, etc.). The worst 28 credits must be subtracted proportionally to the number of validated credits.

(1) Applicants must have graduated by the end of the December Graduation Period
*(2) The weighted average is calculated as follows: ∑(grade*credits) / ∑credits*

2) Applicants from other Italian universities

Applicants who have a Bachelor's degree awarded by another Italian university must have a weighted average grade of all the exams ≥ **24/30**, regardless of the number of years it took them to graduate. The weighted average grade (∑(grade*credits) / ∑credits) is calculated on all accrued course credits (graded on a scale of 30) counting towards the achievement of the Bachelor's degree, after having subtracted the worst 28 credits.

3) Applicants with a non-Italian educational qualification

To be admitted to Politecnico Master's degree programmes, applicants must have an academic qualification awarded by an accredited/recognized foreign university, earned after completing at least 15 years of total education (including primary school, secondary school and university).
Applicants who have attended a university programme lasting five or six academic years (different from the 3+2 system) without completing it must still meet the minimum requirement of 15 years of total education (of which at least 3 years at university level) and they must have earned at least 180 ECTS credits or equivalent. Pre-university courses or foundation years cannot be counted towards the minimum number of credits or the minimum numbers of years of total education mentioned above.
The applicant's academic performance and the consistency between the degree programmes offered by Politecnico and the applicant's previous academic background are assessed by the professors designated by Coordinator of the Collegio. The evaluation is carried out on the Apply@polito platform under the section called "applicants with a non-Italian qualification."

A positive evaluation (offer of admission) allows applicants to enrol in the programme only in the academic year in which the application has been submitted. Admitted applicants who do not complete the enrolment process within the deadlines are required to apply again to the programme in the next academic years.

Students whose native language is not Italian must prove knowledge of the Italian language (minimum A2 level - CEFR) by taking an internal exam organized by Politecnico or by presenting an internationally recognized Italian language certificate. Specific information is available in the Student Guide.

***
More information is available at https://www.polito.it/en/education/applying-studying-graduating/admissions-and-enrolment/master-s-degree-programmes

Art. 3 – Programme curriculum

3.1 Programme overview

Upon first enrolment in the programme, students must indicate the degree class in which they intend to graduate. However, they may change their choice, provided that it becomes final at the time of enrolment in Year 2.

Specifically, the educational path of the Master's degree programme in Cybersecurity Engineering aims to align with major international standards and to be compatible with the competence framework proposed by ENISA ("Cybersecurity Skills Development in the EU"). One of its primary objectives is to make this programme one of the first implementations of the training plan developed by the European Cybersecurity Organisation ("European Cybersecurity Education and Professional Training: Minimum Reference Curriculum," https://www.ecs-org.eu/documents/publications/61967913d3f81.pdf). The programme is designed to provide students with the skills required to address all phases of cybersecurity: identification, protection, monitoring, response, and recovery.

Although the inter-class degree programme is structured as a single programme, the educational path includes four distinct specialist tracks, each corresponding to the professional profiles that the programme aims to train: Cyber Analyst, Cyber Designer, Cryptography Expert and Cyber Legal and Compliance Officer.

Year 1 is common to all tracks. In Year 2, students can tailor their studies by selecting a set of courses aligned with a specific track. The compulsory courses offered in Year 1, considered fundamental for the training of cybersecurity professionals, cover the areas of computer architecture and system programming, network technologies and services, web programming, cybersecurity fundamentals, cryptography, hardware security and wireless communications.

For the Cyber Analyst track, the programme includes courses focused on identifying, managing, and mitigating cyberattacks. The Cyber Designer track offers courses related to the design, coordination, supervision, and implementation of protection technologies and measures. The Cryptography Expert track focuses on modern cryptography, mechanisms, and algorithms that ensure security even in the context of the upcoming quantum transition. In the Cyber Legal and Compliance Officer track students study more in depth legal and managerial aspects, preparing them to assess and manage the compliance of existing or planned security solutions with current standards, legal frameworks, and regulations.

At the end of Master's degree programme students are required to write and defend a written thesis. Students may also do an internship at external companies, research centres or public institutions.

The programme plans to establish agreements with international universities to offer double or joint degrees.

The educational objectives and the expected learning outcomes offer students the tools to either start working in the field of cybersecurity or continue their studies with a PhD programme.

3.2 Organization of educational activities

The list of courses (compulsory and optional), curricula, possible organization of courses into modules, any pre-requisites and exclusions and the list of the faculty members responsible for the courses are available at:

- https://didattica.polito.it/pls/portal30/sviluppo.offerta_formativa_2019.vis?p_a_acc=2026&p_sdu=32&p_cds=468 (LM-32)
- https://didattica.polito.it/pls/portal30/sviluppo.offerta_formativa_2019.vis?p_a_acc=2026&p_sdu=32&p_cds=469 (LM-66 R)

The list of the Scientific Disciplinary Fields (Settori Scientifico Disciplinari) for each activity (specific subjects and complementary subjects) is available at: https://didattica.polito.it/pls/portal30/sviluppo.vis_aig_2023.visualizza?sducds=32468&tab=0&p_a_acc=2026

Art. 4 - Student career

The Student Guide is published on the Teaching Portal every year before the beginning of the academic year. There is a specific Student Guide for each Master's degree programme. The Student Guide is available on the web site of the degree programme.

It contains information and deadlines on:

- academic calendar;
- Personal Study Plan and Annual Personal Study Plan;
- free choice credits;
- internships;
- tuition fees;
- dual career;
- classes and exams;
- class delivery;
- foreign language learning;
- studying abroad/mobility programmes;
- exam rules;
- transfers in/out and internal transfers;
- interruption, suspension, withdrawal, forfeiture;
- credit transfer.

Art. 5 - Final Examination

Students can complete the final examination by choosing between two options: a 22-credit thesis or a 10-credit internship and a 12-credit thesis.

The Final Examination (either the 22-credit or 12-credit option) typically focuses on an innovative analysis, project, or application, related to topics consistent with the educational objectives of the degree programme. It should reflect the candidate's individual contribution and result in a final written report (Master's thesis). The courses offered in Year 2 are organized in a way that leaves a sufficient time for the development of the thesis. The Master's thesis represents a comprehensive assessment of the student's mastery of technical content, as well as organizational, communication, and individual skills, in the context of developing complex analyses or projects. The final examination typically requires the application of knowledge gained from multiple courses, the integration of additional elements and the ability to propose innovative ideas.

If students choose the final examination option consisting of a 12-credit thesis and a 10-credit internship, they will do a curricular internship that enhances their education through on-the-job training in a company, research institution or public administration. The extensive network of contacts that the Departments of Politecnico have with national and international companies, research organizations, and public institutions guarantees a wide range of internship opportunities.

The final examination is worth 12 or 22 credits, corresponding to a period of time ranging from approximately three months to one semester of full-time work.

The topic and activities connected with the thesis must be agreed upon with a faculty member from the Politecnico (thesis supervisor). Students are allowed to work at their thesis project also at external organizations or companies, in Italy or abroad, under the supervision of a thesis supervisor from Politecnico and a tutor from the external institution.

Students who have earned at least 48 credits must submit their thesis application and request the thesis topic online through a dedicated procedure available in their personal page on the Teaching Portal, under the section entitled "Thesis," in compliance with the Graduation Periods deadlines published in the Student Guide – Thematic Calendar Section.

Students are required to publicly present and discuss the preparation activities for their thesis and the corresponding results (oral defence) in front of a Graduation Examining Committee, who will evaluate both the work carried out and the presentation. The Master's thesis and its oral defence must be in English.

The Graduation Examining Committee gives the final grade evaluating the student's overall academic path, his/her maturity, capacity for intellectual reasoning and the quality of the thesis.

The members of the Graduation Examining Committee evaluate the overall average grade of all the exams on a scale of 110. The committee may add up to a maximum of 8 points, considering the following factors:

- quality of the thesis work (commitment, autonomy, methodological rigor, relevance of results achieved, etc.);
- thesis oral defence (clarity in presentation, etc.);
- outstanding results achieved during the academic path (number of honours, time to graduation).

A degree with honours (lode) may be awarded at the Committee's discretion if the total score is at least 112.51.

If the thesis meets the required standards, the Committee may grant the dignità di stampa (printing honour) only if the final grade is 110 cum laude and the Committee's decision is unanimous.

More Information and Deadlines:

- Student Regulations
- Student Guide

Diploma Supplement:
In compliance with article 11, paragraph 8, of Ministerial Decrees No. 509/1999 and 270/2004. Politecnico di Torino issues the Diploma Supplement, a document that can attached to a higher education qualification. It is designed to improve the transparency of international qualifications, as it provides the description of the curriculum successfully completed by the student. This certificate follows the European model developed by the European Commission, the Council of Europe and UNESCO – CEPES: it is issued in two languages (Italian-English) and it is composed of approximately 10 pages.

More information at https://www.polito.it/en/education/applying-studying-graduating/academic-experience/certificates-and-other-documents

Art. 6 - References

6.1 Student Regulations

The Student Regulations define the rights and responsibilities of students and set out the administrative and disciplinary rules that all students enrolled in a degree programme or in a single learning activity at Politecnico must abide by.

6.2 Other Regulations

Particular aspects of students' academic progress are governed by specific Regulations or Calls for Applications published on its website.
In particular:

- The Tuition Fee Regulations specify the annual tuition fees that students must pay. The procedure for requesting a tuition fee reduction is explained in a dedicated guide.
- The University Regulations on Funds for Student Mobility Abroad outline the principles and rules for awarding and disbursing mobility grants. Standard procedures apply to all types of mobility programmes with unified Calls for Applications published twice a year at https://www.polito.it/en/education/applying-studying-graduating/studying-abroad
- The Code of Ethical Conduct also applies to students.