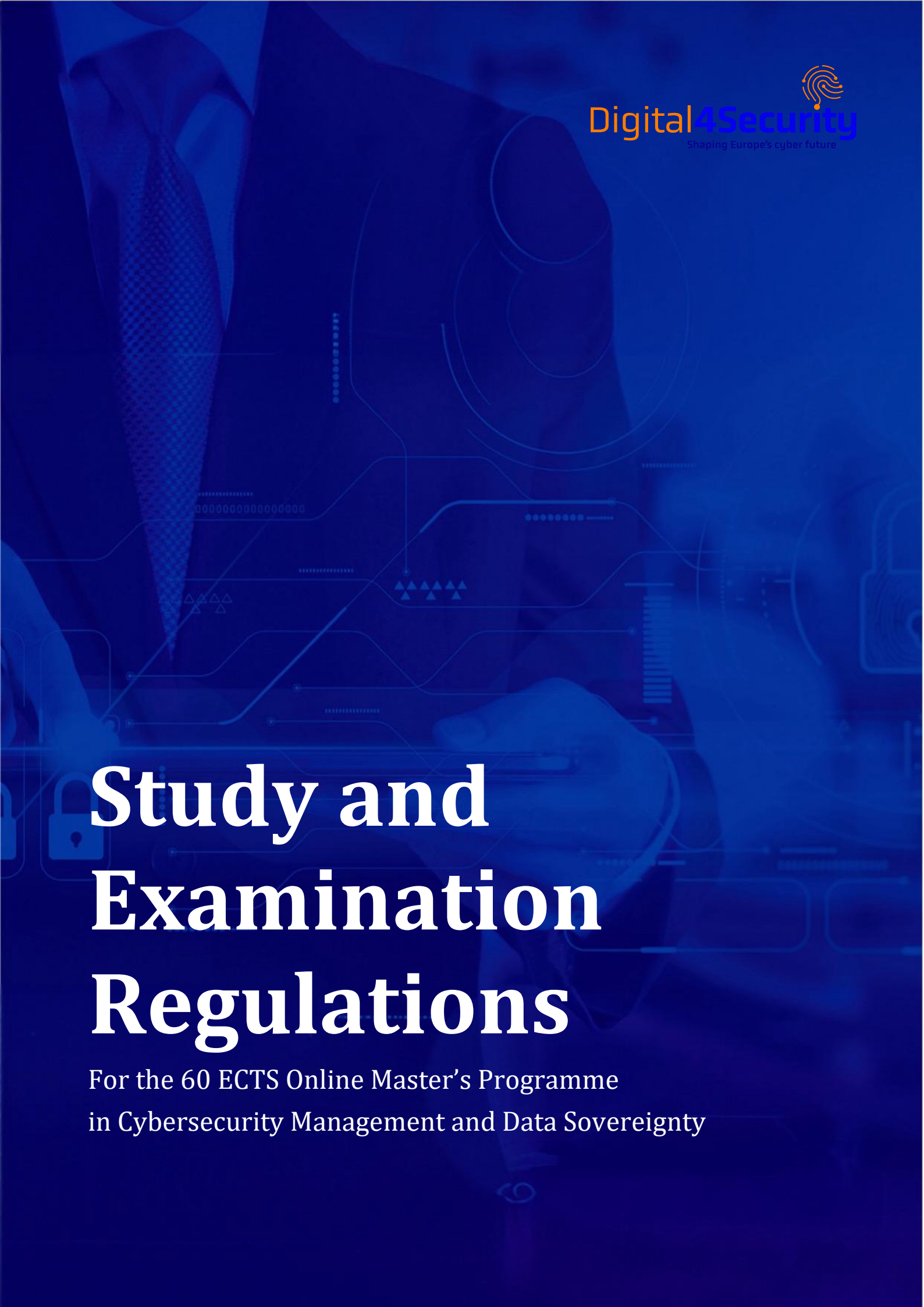


Digital4Security
Shaping Europe's cyber future

Study and Examination Regulations

For the 60 ECTS Online Master's Programme
in Cybersecurity Management and Data Sovereignty

Table of Contents

Introduction

The Joint Master's Programme in **Cybersecurity Management and Data Sovereignty** is a 60 ECTS, fully online degree jointly awarded by the German University of Digital Science (UDS, Germany), Munster Technological University (MTU, Ireland), and Universidad Internacional de La Rioja (UNIR, Spain).

The programme has been created within the framework of the **Digital4Security** project (Grant Agreement No. 101123430), co-funded by the European Union under the DIGITAL Europe Programme (DIGITAL-2022-SKILLS-03 – Advanced Digital Skills).

Designed to meet Europe's growing demand for strategic cybersecurity expertise, the programme combines academic excellence with strong industry relevance. It supports professionals in developing the advanced competencies required to lead cybersecurity efforts across public and private sectors, particularly in Small and Medium-Sized Enterprises (SMEs) and critical infrastructure domains.

These **Study and Examination Regulations** outline the academic framework, assessment principles, and degree requirements that apply to all students enrolled in the 60 ECTS Online Joint Master's Degree Programme in Cybersecurity Management and Data Sovereignty. They ensure transparency, comparability, and academic integrity across the three awarding institutions and serve as a binding reference for students, faculty, and administrative staff.

About the Digital4Security Project

The Joint Master's Programme in **Cybersecurity Management and Data Sovereignty** is delivered collaboratively by the German University of Digital Science (Coordinating Institution, UDS, Germany), Munster Technological University (MTU, Ireland), and Universidad Internacional de La Rioja (UNIR, Spain). The programme has been developed with the support and inspiration of a broad pan-European partner network established through the **Digital4Security** project.

The EU-co-funded Digital4Security project aims to develop innovative, effective, and sustainable master's-level education to cultivate cybersecurity professionals across Europe. This initiative addresses the urgent demand for cybersecurity expertise within European Small and Medium Enterprises (SMEs) and other organizations, striving to protect industries from cyber-attacks and preserve economic stability. The project's core objective is to create one or more innovative European Master's Programmes, equipping graduates with the technical, regulatory, and managerial skills necessary to address both current and emerging cyber threats.

The project is aligned with the goals of the DIGITAL Europe Programme, promoting the development of a robust graduate pool through a dynamic stakeholder ecosystem that includes Higher Education Institutions (HEIs), Research Centres, Employment Services, and industry partners. Specifically, D4S fosters education that integrates academic content with industry insights to rapidly prepare students for high-demand cybersecurity roles, such as Cybersecurity Risk Manager and Chief Information Security Officer (CISO).

Table 1 outlines the partners involved in the Digital4Security project.

Table 1: The Digital4Security Network – Higher Education Institutions (HEIs) and Associate Partners (Listed Alphabetically)

No.	Partner	Abbreviation	Country	Role
1	Adecco Formazione SRL	ADECCO TRAINING	Italy	Associate partner
2	Adecco Italia Holding di Partecipazione e Servizi SPA	ADECCO GROUP	Italy	Associate partner
3	Adecco Italia	ADECCO ITALIA	Italy	Associate partner
4	Ataya & Partners	ATAYA	Belgium	Associate partner
5	Banco Santander SA	BANCO SANTANDER	Spain	Associate partner
6	Brno University of Technology	BRNO	Czech Republic	HEI partner
7	Cefriel Società Consortile a Responsabilità Limitata Società Benefit	CEFRIEL	Italy	Associate partner
8	CMIP (Polski Klaster Cyberbezpieczenstwa CyberMadeInPoland Sp. z o. o.)	CMIP	Poland	Associate partner
9	Contrader SRL	CONTRADER	Italy	Associate partner
10	CY Cergy Paris Université	CY	France	HEI partner
11	Cyber Ranges Ltd	CYBER RANGES	Cyprus	Associate partner
12	DigitalEurope AISBL	DIGITALEUROPE	Belgium	Associate partner
13	Digital Technology Skills Limited	DTSL	Ireland	Associate partner
14	European Digital SME Alliance	DIGITAL SME	Belgium	Associate partner
15	Fraunhofer Gesellschaft zur Förderung der Angewandten Forschung EV	FHG	Germany	Associate partner
16	German University of Digital Science	UDS	Germany	HEI partner
17	Independent Pictures Limited	INDIEPICS	Ireland	Associate partner
18	IT@Cork Association Limited LBG	IT@CORK	Ireland	Associate partner
19	Matrix Internet Applications Limited	MATRIX	Ireland	Associate partner
20	Munster Technological University	MTU	Ireland	HEI partner

No.	Partner	Abbreviation	Country	Role
21	Mykolo Romerio Universitetas	MRU	Lithuania	HEI partner
22	National College of Ireland	NCI	Ireland	HEI partner
23	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	NASK	Poland	Associate partner
24	Pearson Benelux	PEARSON B.	Netherlands	Associate partner
25	Politecnico di Milano	POLIMI	Italy	HEI partner
26	Profil Klett d.o.o.	PROFIL KLETT	Croatia	Associate partner
27	Red Open S.R.L.	RED OPEN S.R.L.	Italy	Associate partner
28	Schuman Associates SCRL	SA	Belgium	Associate partner
29	ServiceNow Ireland Limited	ServiceNow	Ireland	Associate partner
30	Skillnet Ireland Company Limited By Guarantee	SKILLNET	Ireland	Associate partner
31	Terawe Technologies Limited	TERAWE	Ireland	Associate partner
32	Universidad Internacional de La Rioja	UNIR	Spain	HEI partner
33	Università degli Studi di Brescia	UNIBS	Italy	HEI partner
34	Universitatea Națională de Știință și Tehnologie Politehnica București	UPB	Romania	HEI partner
35	Universität Koblenz	UNI KO	Germany	HEI partner
36	University of Rijeka	UNIRI	Croatia	HEI partner
37	Vytautas Magnus University	VMU	Lithuania	HEI partner

The training programmes developed through the Digital4Security project focus on cybersecurity management education at Master's level, utilizing upskilling and reskilling approaches. Educational offerings combine managerial and technical content to meet industry needs with an emphasis on cultivating advanced leadership skills in cybersecurity. Graduates will be equipped to critically assess cybersecurity principles, technologies, and practices, enabling them to lead cybersecurity efforts within modern organizations, while also ensuring legal compliance.

With a strong focus on practical application, the educational offerings blend academic theory with real-world industry expertise to ensure that graduates are not only knowledgeable, but also employment ready. Supporting this approach, the Digital4Security project encourages the attainment of industry-recognized certifications as a core element of the learning journey. In addition, students benefit from mentoring opportunities and project-based learning in collaboration with industry partners, enhancing their skills in real-world cybersecurity contexts.

The educational approach caters to diverse learner audiences by offering tailored programmes implemented by collaborating institutions. These programmes aim to create a large pool of up-to-date, market-relevant content, following effective teaching strategies that enhance student empowerment and career prospects. Specifically, the Digital4Security project sets out to offer:

- A 120 ECTS hybrid master's programme, designed for recent graduates, led by the University of Bucharest.
- A 60 ECTS online master's programme for learners with industry experience, available in full-time and part-time options, led by the German University of Digital Science.
- Micro-credential courses that can be stacked and recognized in the master's programmes.
- Various events and networking opportunities such as weekend lectures.

All programmes benefit from a shared pool of high-quality resources made available to all partner institutions, supporting the design, delivery, and management of educational offerings. These shared assets include, but are not limited to:

- A Digital4Security Platform Infrastructure
- Outreach and Communications Support
- A Train-the-Trainer Program
- Branded Course Templates and Consistent Learning Frameworks
- An Academic Collaboration Network
- Engagement with the Digital4Security Industry Advisory Board
- A Research and Insight Repository

While all Digital4Security (D4S) programmes benefit from the insights, infrastructure, and resources developed in the EU co-funded project, each academic offering is designed to be self-contained and sustainable beyond the EU-project's lifecycle. Two distinct master's programme formats have emerged from the Digital4Security (D4S) initiative, tailored to different learner audiences. Table 2 highlights both the commonalities and differences between the 60 ECTS Online Programme and the 120 ECTS Hybrid Programme in Cybersecurity Management and Data Sovereignty, each developed and offered by a different group of collaborating Higher Education Institutions.

Table 2: Comparison of the 60 ECTS Online Master's and the 120 ECTS Hybrid Master's Programmes Developed under the Digital4Security Initiative (italics indicate differences)

Factor	60 ECTS Online Programme	120 ECTS Hybrid Programme
Target Audience	*Mid-career professionals with managerial experience or aspirations*	*Graduates or early-career professionals*
Entry Requirements	Bachelor's degree (in any field); English proficiency (min. B2)	Bachelor's degree (in any field); English proficiency (min. B2)
Delivery Mode	*Fully online*	*Hybrid (combining online and on-campus learning)*
Priorities	*Flexibility for working professionals; concise education*	*In-depth content; PhD preparation; integrating local culture*
Duration (Full-Time)	*1 year*	*2 years*
ECTS Credits	*60*	*120*
European Qualifications Framework	EQF Level 7 (Master's)	EQF Level 7 (Master's)
Degree Awarded	Master of Science (MSc)	Master of Science (MSc)

The Study and Examination Regulations outlined in this manual apply to the **60 ECTS Online Joint Master's Degree Programme** in Cybersecurity Management and Data Sovereignty, which is collaboratively developed, coordinated, and delivered

by three partner institutions: the German University of Digital Science (Coordinating Institution, UDS, Germany), Munster Technological University (MTU, Ireland), and Universidad Internacional de La Rioja (UNIR, Spain).

1. Admission and Minimum Entry Requirements

Applications for admission to the 60 ECTS fully online Joint Master's Programme in Cybersecurity Management and Data Sovereignty are submitted via the centralised online application portal, accessible through the Digital4Security website: **www.digital4security.eu**. The application process follows a biannual intake cycle. Deadlines are published in advance, with dates determined by the Master's Board of Directors, where feasible, one year in advance.

The Joint Admissions Board, composed of at least one representative from each partner institution, is responsible for ensuring that all applicants are assessed fairly and transparently.

Minimum entry requirements:

- A Bachelor's degree (EQF Level 6, or national equivalents) in any discipline; and
- English language proficiency at CEFR level B2 or above, as detailed in Section 1.2.

In addition, all students must have appropriate technical equipment to participate in a fully online programme, as detailed in Sect. 1.3.

Admission is open to graduates from both technical (e.g. computer science, data science) and non-technical backgrounds (e.g. economics, law, business). The programme is particularly suited for applicants with professional experience or aspirations in leadership, technical, or compliance-related roles.

During the runtime of the Digital4Security project, European students benefit from 50% funding of tuition fees. This support applies only to students who hold citizenship of an EU Member State. During the admission process, all applicants are required to upload a valid passport or travel document for identity verification. This document also serves as proof of eligibility for reduced admission fees among European citizens.

Applicants who have not yet formally obtained their Bachelor's degree at the time of application may be considered for conditional admission. To be eligible, applicants must submit a declaration from their current university confirming that all degree requirements will be fulfilled prior to the commencement of the Master's Programme. All required documentation – including the final Bachelor's degree certificate and any additional materials necessary to meet the programme's entry requirements – must be submitted in full before the official start of the programme.

Late applications may be considered at the discretion of the Joint Admissions Board, subject to availability of places and the timely submission of all required documentation.

1.1 Necessary Documentation for Application

To support a streamlined and accessible admissions process, applicants are asked to submit a lean set of documents sufficient to verify eligibility and to understand their context and motivation for applying.

All applications must be submitted via the programme's application portal, following the published deadlines and instructions. A complete application must include the following documents:

- A copy of the applicant's passport or travel document (main identity page only);
- A certified copy of the Bachelor's diploma (EQF Level 6, or national equivalents), with an official English translation if the original is not in English;
- If available, a copy of the Diploma Supplement;
- Certified academic transcripts, with official English translations where applicable;
- Proof of English language proficiency;
- A brief Curriculum Vitae in English, preferably using the **Europass** format;

- A personal statement (approx. 300–500 words) outlining the applicant's motivation and professional goals.

Supplementary documents may only be requested by the Joint Admissions Board where strictly necessary for final admission decisions.

By submitting an application, candidates confirm that all provided information is accurate, and consent to the processing of personal data for admission purposes.

1.2 Language Qualification Requirements

As the programme is delivered entirely in English, all applicants must demonstrate sufficient English language proficiency to participate effectively in coursework, group activities, and assessments.

Applicants can demonstrate English language proficiency through one of the following:

- **Applicants whose first language is English**
  Must indicate this in the application form and may be asked to provide supporting evidence, such as school-leaving qualifications or other relevant documentation, if clarification is needed.
- **Applicants who have completed a previous school or university degree taught fully in English**
  Must provide a formal statement or certificate from the awarding institution confirming that the programme was taught in English, or submit a Diploma Supplement or transcript indicating English as the language of instruction.
- **Applicants with at least 2 years of relevant professional experience in an English-speaking context**
  Must submit documentation confirming that English was the primary working language. This can be a signed letter from an employer, on official letterhead, stating the applicant's role, period of employment, and that

English was the primary language used in daily professional communication.

Applicants who do not fall into any of the above categories are required to submit an official English language test certificate meeting the programme's minimum standards, as shown in Table 3.

Table 3: Minimum Language Proficiency Requirements

Test Type	Minimum Score	CEFR Level
IELTS (Academic)	6.5 overall	B2
TOEFL iBT	79	B2
TOEFL PBT	550	B2
TOEFL CBT	213	B2

Test certificates must be valid (issued within the last two years) and verifiable at the time of application. Applicants are only required to submit one form of evidence to meet the language prerequisites.

1.3 Required Equipment

To successfully participate in an online study programme, students must ensure access to essential equipment and infrastructure. By successfully completing the application process via the online platform, students demonstrate that these conditions are met initially.

The following equipment is required:

- **Laptop or Desktop Computer, or equivalent:** Capable of running video conferencing tools, accessing cloud-based learning platforms, and using standard productivity software.

- **Internet Connection:** Stable and fast enough to stream lectures, join live seminars, and upload assignments.
- **Webcam and Microphone:** Required for oral assessments and interactive sessions.
- **Controlled Study Environment for Exams:** During assessments, students must ensure they are in an interruption-free space where no individuals, animals, or objects can enter or interfere in an uncontrolled manner.

These requirements are outlined in the Student Agreement, with students confirming their compliance by signature as a prerequisite for enrolment.

Further recommendations and guidance on learning tools and environments are provided in the *Student Handbook* (Annex 8).

1.4 Recognition of Prior ECTS

Students may apply for the recognition of prior academic achievements within the 60 ECTS Online Master's Programme, following the procedures outlined in Sections 1.4.1 and 1.4.2. Other forms of Recognition of Prior Learning (RPL) that fall outside these provisions are not eligible.

Applicants may already be admitted to the programme by the Joint Admissions Board while requests for recognition of ECTS are still pending review.

The programme entry requirements and policy for recognition of prior learning have been harmonised across the various offerings within Digital4Security to support seamless student mobility. In particular, students who complete the 60 ECTS online Master's may subsequently apply to the 120 ECTS hybrid Master's to earn additional ECTS in the subject domain, as may be required for PhD enrolment. The programme's entry requirements have been designed to ensure that students who meet the enrolment prerequisites of the shorter 60 ECTS programme also fulfil the enrolment criteria for the longer 120 ECTS programme.

1.4.1 Micro-Credential Recognition

Micro-credentials may be eligible for academic recognition under the following conditions:

- Micro-credentials and degrees issued under the Digital4Security programme will be recognised according to their assigned ECTS value. These qualifications are awarded by higher education institutions participating in the Digital4Security project and are directly linked to the Digital4Security initiative. The corresponding micro-credential offerings are officially listed on the Digital4Security website. In most cases, enrolment in these micro-credentials or degrees will have been initiated via the Digital4Security website and can be internally verified.
- Certificates aligned with the European Digital Credentials for Learning (EDCI) standard may also be accepted directly according to their ECTS value, provided they are aligned with the programme's learning outcomes.
- Other formats – such as nationally accredited courses, certificates, or open badges – will be reviewed by the Examinations Board for potential recognition. Recognition requires clear alignment with the programme's learning outcomes, verifiable information on workload, and demonstrably high academic standards in the evaluation of student achievement.
- Up to 15% of the total programme ECTS, equivalent to 9 ECTS, may be recognized from micro-credentials and degrees, counting towards the Joint Master's degree.

Applicants who already hold relevant micro-credentials at the time of application to the Master's Programme may request ECTS recognition by completing the Micro-Credential Recognition Form as part of the admissions process.

Students who obtain a qualifying micro-credential after programme enrolment, or who wish to apply for recognition at a later stage, may submit their request by contacting **secretariat@digital4security.eu**. Such recognition requests will only be accepted during the designated processing window, which is limited to the **first**

two weeks of any active term. Requests must be submitted while the student is still enrolled in the programme and has not yet completed their studies.

Automatic recognition of D4S credentials is confirmed by the Secretariat, within the limit of 9 ECTS that students may earn via micro-credentials. Applications based on EDCI or other formats, or purported D4S certificates involving uncertainty, are referred to the Examinations Board for review.

ECTS credits recognized through micro-credentials or degrees within the Master's Programme count towards **elective study options**, and are documented accordingly in the Diploma Supplement, unless a student completed a mandatory programme module via microcredential enrolment (cf. *Student Handbook*, Annex 8).

1.4.2 Programme Re-Enrolment and Recognition of Previously Completed ECTS

Students who have previously completed ECTS credits within the Master's programme and subsequently unenrolled prior to completing the full degree may apply to re-enrol at a later date. In accordance with the *Cooperation Agreement* (Annex 1), such students shall be given priority in the admission procedure, as they retain the right to re-enter the programme with full recognition of completed modules, unless substantial grounds preclude this.

Upon re-enrolment:

- The ECTS credits previously earned will be fully recognised, provided they remain compatible with the current programme structure and learning outcomes.
- Re-enrolment is subject to the terms, conditions, fee structure, and curricular framework in effect at the time of the new enrolment.

If the core curricular structure has not changed since the last enrolment, the Secretariat may automatically recognise all previously completed components. If

the curriculum has changed – particularly through reaccreditation and structural revisions – the Examinations Board shall review and confirm the recognition of prior academic achievements from the previous enrolment.

For all students seeking re-enrolment, admission is only possible if the applicant is eligible to complete the full programme under the current regulations. Students who have previously failed a required module or assessment the maximum number of permitted times (as outlined in Section 6.4.3) are not eligible for re-admission, unless the programme structure has been revised through reaccreditation and the failed component is no longer mandatory.

Students who were previously expelled from the programme due to severe academic misconduct lose the right to re-enter at a later stage. While re-admission is not categorically excluded, such applicants shall not be given priority, and any recommendation for re-admission by the Admissions Board must be formally approved by the Master's Board. If recommending re-admission, the Admissions Board must provide a substantiated justification, such as evidence of a procedural error or unfounded accusations that led to the original expulsion.

1.5 Application Review Procedure

The Secretariat performs an initial check for completeness and requests any missing documents from applicants via the platform.

Complete applications, including all the minimum required components, are marked for review by the Joint Admissions Board.

Each application is reviewed by representatives of all three awarding partners. Admission requires the confirmation of eligibility by all three partners.

In accordance with the *Cooperation Agreement* (Annex 1), no partner institution shall be required to admit a student if such admission would violate national legal or regulatory requirements applicable to that institution. If a student cannot be

legally admitted by one of the three degree-awarding universities, the student shall not be admitted to the Joint Degree Programme.

Members of the Joint Admissions Board shall conduct reviews generously, with the aim of admitting all applicants who have submitted the required documentation, are formally admissible, and for whom no significant grounds for rejection exist.

The Joint Admissions Board notifies the Master's Board (**masters.board@digital4security.eu**) and the Secretariat (**secretariat@digital4security.eu**) of the list of all admitted candidates. Where candidates cannot be admitted, a brief explanation must be provided. The Secretariat ensures timely implementation of the decisions on the platform, enabling admitted students to proceed with signing their Student Agreement and submitting payment to enrol in the programme.

1.6 Rejection Appeals

Applicants wishing to contest a negative admission decision may submit a written appeal within 14 calendar days of receiving the official rejection result. Appeals should be emailed to **admissions@digital4security.eu**, with **secretariat@digital4security.eu** copied in cc.

Appeals must clearly state the grounds for re-evaluation, such as documents not considered or misunderstood, and may include additional supporting documentation. Appeals based on challenging the programme's established admission criteria may be desk-rejected. All other appeals will be reviewed by the Admissions Committee, which will provide a final, reasoned response, typically within four weeks.

1.7 Student Agreement

All admitted students must enter into a Student Agreement prior to enrolment. The Agreement, authorised by the Master's Board, sets out the mutual rights and obligations of the student and the degree-awarding universities. This includes compliance with the Study and Examination Regulations. Special emphasis shall be placed on adherence to academic integrity and ethical conduct, fulfilment of technical and equipment requirements, and the student's commitment to active participation in all required learning activities, assessments, and quality assurance processes.

The fee structure shall be specified, with clearly outlined consequences in the event of payment failure. By their signature, students commit to timely payment.

The data protection principles of the programme shall be outlined, including compliance with the General Data Protection Regulation (GDPR). Synchronous study sessions may be recorded to ensure content access for students unable to attend live. By signing, students consent to the processing of their personal data in accordance with the stated regulations.

Furthermore, the Student Agreement shall include provisions on liability, clarifying the extent to which the degree-awarding universities may be held responsible for their performance of obligations, and limiting liability in accordance with applicable law. It shall also specify the competent jurisdiction and applicable law for the resolution of disputes, taking into account the joint nature of the programme and the national legal requirements of the partner institutions.

The process of issuing and signing the Student Agreement shall be implemented through the programme's CRM system (Full Fabric), ensuring GDPR-compliant, secure handling and documentation. The Agreement forms a binding part of the contractual relationship between the student and the partner institutions and remains in force for the duration of enrolment.

1.8 Microcredentials and Admission Prerequisites

Modules that form part of this Master's programme may also be offered and certified as microcredentials. This means that the participant group in a module may be mixed, comprising students already enrolled in the full Master's programme and learners admitted only to a single module as a microcredential. The latter option enables participants, for example, to explore the programme before committing to full enrolment. Where a learner subsequently applies for admission to the Master's programme, one module successfully completed as a microcredential can be recognised as prior learning, in accordance with Section 1.4 of the *Study and Examination Regulations*.

Different admission criteria may apply depending on whether students enrol for the full Master's programme or for a single module. Submission of a bachelor's degree and other formal documentation is typically required only for full programme admission.

However, the academic prerequisites for participation in a module are identical for all students, regardless of the enrolment route. Where the *Module Handbook* (Annex 7) specifies that knowledge, skills and competencies from Module A are required for enrolment in Module B, these qualifications must be demonstrated, but not necessarily through completion of Module A. Applicants for microcredentials may alternatively submit evidence of other academic or professional qualifications that substantiate the prerequisites for admission.

Microcredential applications are managed through the D4S platform infrastructure in the same way as full programme admissions, with the application process initiated via the website. Admission requirements are based on the module prerequisites specified in the *Module Handbook.* In cases where further information shall be provided during the admission procedure, such as recommendations on the type of evidence to demonstrate the necessary knowledge, skills and competencies, formulations shall be provided by the Joint Admissions Board in consultation with the module's main lecturer.

Applications for both single-module admission and full programme admission are processed by the Joint Admissions Board. In cases of uncertainty as to whether microcredential applicants possess the necessary prerequisites for the module in question, the final admission decision may be referred to the module's main lecturer. In exceptional cases where modules are offered as microcredentials independently of the Master's programme, admission decisions rest with the module's main lecturer, while the Joint Admissions Board and the Quality Service Committee oversee the procedure, monitoring shared standards and compliance.

Once admitted to a module, no distinction is made between student populations, whether enrolled in the full Master's programme or as microcredential learners. Although microcredentials may in principle be offered as stand-alone courses beyond the Master's curriculum, the standard arrangement is that Master's modules are additionally opened to microcredential participants. Accordingly, in these cases there is a single course, identical for all learners, including ECTS allocation, intended learning outcomes, study materials, teaching methods, week-by-week structure, examinations, and certification of the completed module.

2. Period of Study

The Joint Online Master's Degree Programme in Cybersecurity Management and Data Sovereignty comprises 60 ECTS. The programme workload is defined using the European Credit Transfer and Accumulation System (ECTS). **One ECTS** credit corresponds to approximately **25 hours of student work**, including all study-related activities such as lectures, readings, assignments, and self-study.

Students may choose from one of three delivery tracks, depending on the level of time commitment they can make and their preferred pace of study:

- **Full-Time Track:** 1 year (3 terms), 20 ECTS per term;
- **Part-Time Accelerated Track:** 1¼ years (4 terms), 15 ECTS per term;
- **Part-Time Track:** 2 years (6 terms), 10 ECTS per term.

These tracks are designed to support flexibility for working professionals while maintaining coherent learning paths. Table 4 summarizes the expected duration and workload for each delivery track.

Table 4: Expected Duration of the Degree Programme across Different Tracks

Programme	Mode of Study	Intake Rhythm	Expected Time to Completion	ECTS per Term
Joint Master's Degree Programme in Cybersecurity Management and Data Sovereignty (60 ECTS, Online)	Full-Time	Twice annually	3 terms / 1 year	20
	Part-Time Accelerated	Twice annually	4 terms / 1¼ years	15
	Part-Time	Twice annually	6 terms / 2 years	10

Students may switch from one track to another. Requests shall be sent to **Secretariat@digital4security.eu**, at least four weeks prior to the start of the next term. Standard track-fees apply. Adjustments to the fee structure will take effect from the date of the change and will not be applied retroactively.

Figures 1-3 provide a comparative overview of the study tracks.

Blue fields indicate taught modules (one cell = 5 ECTS), orange fields highlight the typical thesis period, and white fields represent term breaks.

Figure 1. Full-Time Track (1 Year / 3 Terms / 20 ECTS per Term).

1st Trimester		2nd Trimester		3rd Trimester	
				Thesis (15 ECTS)	
20 ECTS		20 ECTS		20 ECTS	

Figure 2. Part-Time Accelerated Track (1¼ Years / 4 Terms / 15 ECTS per Term).

1st Trimester		2nd Trimester		3rd Trimester	
15 ECTS		15 ECTS		15 ECTS	
4th Trimester					
Thesis (15 ECTS)					
15 ECTS					

Figure 3. Part-Time Track (2 Years / 6 Terms / 10 ECTS per Term).

1st Trimester		2nd Trimester		3rd Trimester	
10 ECTS		10 ECTS		10 ECTS	
4th Trimester		5th Trimester		6th Trimester	
				Thesis	
		Thesis			
10 ECTS		10 ECTS		10 ECTS	

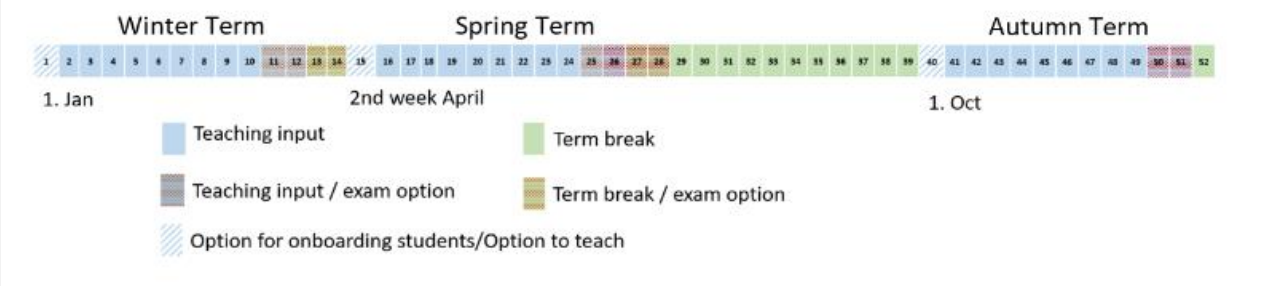
The detailed academic calendar indicating the distribution of workload across the year is presented in Figure 4. Each teaching term has a standard duration of 12 weeks, with the start dates as follows: 1 January for the Winter Term, the second week of April for the Spring Term, and 1 October for the Autumn Term.

Examinations may extend into weeks 13 and 14 in the Winter and Spring Terms. The Autumn Term concludes strictly by the end of week 12, followed by a Winter (Christmas) Break.

Ordinary exams take place during the 12-week teaching period, or in week 13 or 14 where supported by the academic calendar. Extraordinary (repeat) exams take place during the first six weeks of the next teaching term.

A designated Summer Break occurs annually during weeks 29 to 39 (typically covering mid-July through the last week of September). During this period, there are no scheduled classes, examinations, or required coursework, allowing students time for rest, intensified work, internships, or independent study.

Figure 4. The Academic Calendar across Weeks of the Year.



3. Governance of the Joint Programme

The Joint Master's Degree Programme in Cybersecurity Management and Data Sovereignty is governed by a set of bodies established under the *Cooperation Agreement* (Annex 1) between the German University of Digital Science, Munster Technological University, and Universidad Internacional de La Rioja. These governance bodies are responsible for overseeing academic quality, programme administration, and key decision-making processes.

The joint governance structure includes the following bodies:

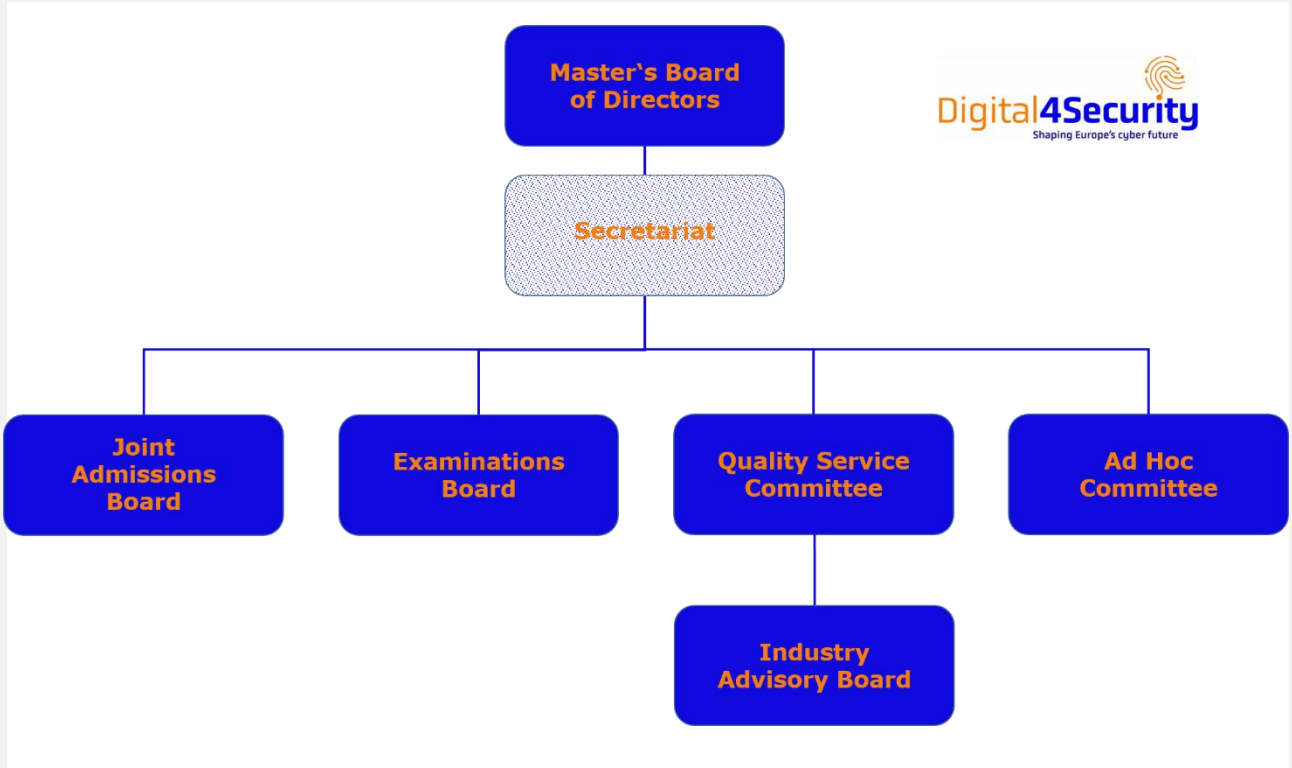
- Master's Board of Directors
- Programme Secretariat
- Joint Admissions Board
- Examinations Board
- Quality Service Committee
- Ad-hoc Committees as needed
- Industry Advisory Board

Each Partner Institution is represented in the joint governance structure, and students may be consulted through representative mechanisms further detailed in the *Student Handbook* (Annex 8).

Fig. 5 provides an overview of the governance structure.

While the Master's Board of Directors constitutes the highest decision-making body within the programme, and the Quality Service Committee plays a key role in upholding academic standards and fostering continuous improvement, the Joint Admissions Board and the Examinations Board are primarily responsible for the implementation of the *Study and Examination Regulations*. Their respective responsibilities are outlined below.

Fig. 5: Basic Governance Structure of the 60 ECTS Online Master's Programme in Cybersecurity Management and Data Governance.



3.1 Joint Admissions Board

The Joint Admissions Board is responsible for the fair, transparent, and academically sound selection and admission of students to the Joint Master's Programme. It ensures that admission decisions are made in accordance with the jointly agreed standards, and in full compliance with the European Approach for Quality Assurance of Joint Programmes.

The Joint Admissions Board:

- Reviews all applications submitted within the defined deadlines;
- Selects and admits students in accordance with the programme's agreed admission criteria;

- Ensures consistency and transparency across all partner institutions;
- May request further information or clarification from applicants where needed;
- May consult academic experts, student services, or legal advisors in complex cases;
- Ensures appropriate documentation of decisions and feedback to applicants.
- Organizes training for all staff on the programme's data protection regulations, including GDPR compliance, and ensures that a designated Data Protection Officer oversees procedures at the partner institutions.

The Joint Admissions Board is standardly composed of one representative from each degree-awarding university. Each partner institution is responsible for appointing its representative in accordance with its own internal procedures and national regulations.

The Board is assisted by the Secretariat and operates under the supervision of the Master's Board of Directors.

Meetings are held:

- At least once after each application deadline;
- As needed until the selection and admission procedure is completed;
- Physically or via digital means, allowing for effective international collaboration;
- With supporting documentation shared in advance and decisions recorded in writing.

In cases where programme updates or legal frameworks affect admission procedures, the Joint Admissions Board coordinates with the Master's Board and relevant institutional offices to ensure compliance and continuity.

3.2 Examinations Board

The Examinations Board is responsible for maintaining the academic integrity and examination standards of the Joint Programme. It ensures that assessments are conducted fairly and consistently across all partner institutions and that students are treated equally under the jointly agreed procedures.

The Examinations Board:

- Oversees examination and assessment procedures;
- Monitors and ensures compliance with institutional, regional, national, and European Union requirements relating to assessment, including requirements related to joint academic standards and the European Approach for Quality Assurance of Joint Programmes.
- Upholds principles of transparency, fairness, and consistency in all grading and assessment practices, ensuring that all students are treated equally and in accordance with the agreed academic standards and quality assurance policies.
- Approves grades and manages grade conversion across systems;
- Reviews and rules on special cases (e.g., suspected misconduct, appeals, or exceptional re-assessment requests);
- May authorize deviations or additional attempts in justified exceptional cases.

The Examinations Board is chaired by the Master's Board of Directors and may include additional members from partner institutions, especially those with expertise in examination administration and quality assurance.

Meetings are held:

- After each formal examination period;
- As needed for urgent matters via digital communication;
- With a minimum one-week notice unless urgency demands expedited consultation;

- With supporting documentation shared in advance and decisions recorded in writing.

All assessments are conducted in accordance with consistent grading criteria. The joint grading scale, including the grade conversion table used across all partner Institutions, is defined in Section 5 (Grading System).

3.3 Student Representation

Students of the Joint Master's Programme have the right to participate in the continuous quality assurance and programme development through elected representation.

Student representatives may be nominated to serve as voting members of the Quality Service Committee. These representatives play an active role in contributing to discussions and formulating recommendations related to academic quality, student experience, and programme enhancement.

The nomination process, term of office, roles, and responsibilities of student representatives are detailed in the *Student Handbook* (Annex 8). All students will be informed of the nomination process at the start of their studies and given an opportunity to participate.

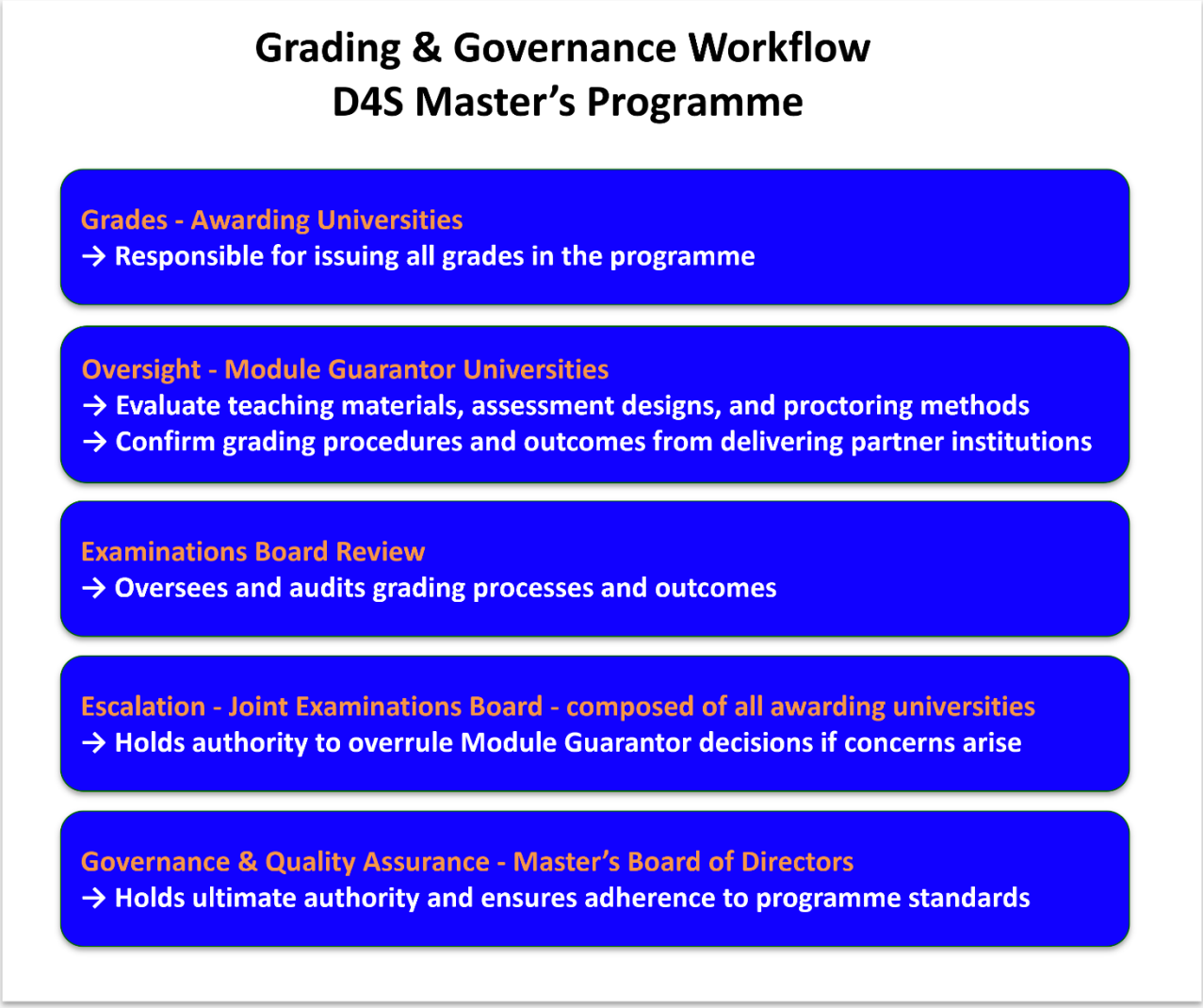
3.4 Assessment and Grading Quality Assurance

The following order of precedence applies: The awarding universities are responsible for issuing all grades in the programme. Where applicable, the awarding universities act as Module Guarantor institutions, confirming the grading procedures and outcomes of delivering partner institutions from the Digital4Security network. The Examinations Board oversees all grading processes and may, where appropriate, audit grading procedures and outcomes. Should any concerns arise, the Joint

Examinations Board (comprising all awarding partners) has the authority to overrule decisions made by Module Guarantor institutions. The Master's Board of Directors holds ultimate authority and responsibility for ensuring adherence to programme standards.

This procedure is illustrated in Figure 5.

Figure 5: Grading Quality Assurance Workflow.



3.4.1 Pre-Delivery Review of Assessment Design and Procedures

Grading oversight shall focus on the assessment tasks, grading criteria and procedures used ahead of module delivery and grading. Reviews may draw extensively on the toolbox for Module Guarantor institutions in the *Programme Survey Scales* (Annex 5), applicable to both delivering and awarding partner module reviews. Any relevant additional data available through the programme's quality assurance procedures, as defined in the *Internal Quality Handbook* (Annex 4), shall also be taken into account. Grades duly issued in accordance with the module's confirmed assessment procedures should ordinarily not be altered, unless there is substantiated evidence of academic misconduct affecting the task performance, or there are other significant reasons. All relevant bodies and individuals shall coalesce to ensure that grades displayed on the learning platform are reliable and valid, with oversight systematically addressing all aspects of assessment design and grading, and with final confirmation and issuance of grades taking place in a timely manner.

Complementing these grading quality assurance measures, assessor requirements defining the minimum qualifications for module instructors and examiners are specified in Section 3.5.

3.4.2 Alignment of Module Guarantor Reviews

The Examinations Board is responsible for ensuring that assessment procedures across all partner institutions are consistent with jointly agreed programme standards. This includes oversight of Module Guarantor reviews, which are conducted in line with QAP.05 of the *Internal Quality Handbook* (Annex 4) and informed by the analysis tools provided in the *Programme Survey Scales* (Annex 5).

In this process, awarding institutions review modules delivered by higher education partners from the Digital4Security network, including the proposed assessment procedures, and submit their evaluations to the Quality Service Committee.

Where possible, Module Guarantor reviews should be carried out by ordinary members of the Examinations Board to promote shared expertise and consistent interpretation of standards.

The Quality Service Committee shall verify the submitted evaluations for cross-institutional consistency and alignment with programme standards. Where significant divergences in assessment approval or grading practices are identified, the matter shall be referred to the Examinations Board. The Board may then take action as appropriate, which can include convening an extraordinary meeting of representatives from all awarding partners to resolve discrepancies and confirm aligned procedures.

3.5 Instructor Requirements

The main instructor responsible for delivering a module in the Joint Master's Programme in Cybersecurity Management and Data Sovereignty must meet the following minimum requirements:

- **Academic Qualification**: Instructors must hold a doctoral degree (PhD or equivalent) in a discipline relevant to the subject area of the module they are assigned to teach. (Exceptions may be granted by the Master's Board in the case of outstanding lecturer experience, but for a maximum of 4 out of the programme's 24 modules.)
- **Language Proficiency**: As the programme is delivered entirely in English, instructors must demonstrate a high level of English language proficiency, both in written and spoken form, to ensure clarity and accessibility in teaching.
- **Pedagogical Approach**: Instructors are expected to adopt a student-centred teaching philosophy that supports active engagement, inclusivity, and responsiveness to diverse learner needs.

Supportive teaching staff, such as tutors or facilitators, must likewise demonstrate English proficiency and follow a student-centred approach, although they are not required to hold a doctoral degree.

Across all modules, at least 50% of the main instructors shall hold the academic title of professor. Any exemptions to this target must be formally approved by the Master's Board and shall be granted only on a term-limited or temporary basis. In such cases, the Master's Board shall take appropriate action to ensure timely progress towards meeting the target. This may include consultation with delivering partner institutions from the Digital4Security network and clear communication regarding the importance of maintaining a high proportion of instructors with senior academic standing.

The main module instructor also serves as the module examiner, responsible for implementing assessments and grading procedures in line with the programme's standards and the confirmed approaches. Instructors from delivering partner institutions are required to follow the procedures agreed with and confirmed by the Module Guarantor institution.

3.6 Supporting Instructional Quality via Data Analysis

The quality of module delivery is monitored through a systematic and data-informed quality assurance process. Two key instruments are employed:

- The *Internal Quality Handbook* (Annex 4) provides a detailed framework for academic monitoring, including metrics such as course progression analysis and automated evaluations of teaching materials.
- The *Programme Survey Scales* (Annex 5) collect detailed student feedback each term on multiple aspects of teaching quality, such as:

    - Clarity and structure of the module;
    - Understandability of the lecturer's spoken English and presentation materials;

- Delivery style and level of interactivity;
- The professionalism and conduct of the instructor towards the students.

The Quality Service Committee is responsible for systematically reviewing the resulting quality assurance data. It identifies any concerns requiring follow-up, supports targeted interventions where necessary, and highlights exemplary teaching practices. Recognised "best cases" are shared across the teaching team to support ongoing professional development. The Committee also ensures that selected best practice examples and related recommendations are progressively integrated into the *Practical Guide for Lecturers* (Annex 10). Further details regarding the Quality Service Committee, its review procedures, and related activities are provided in the *Internal Quality Handbook*.

Instructors are expected to build on the guidance provided by the Quality Service Committee, and to consult the *Practical Guide for Lecturers* (Annex 10) to continuously enhance their teaching.

4. Curriculum and Modules

4.1 Programme Structure

The Joint Master's Degree Programme in Cybersecurity Management and Data Sovereignty is a fully online programme comprising a **total of 60 ECTS credits**. It is designed to support professional learners through modular, flexible pathways while maintaining academic coherence and quality.

The programme is structured as follows:

- **30 ECTS – Compulsory Components:**
  - *15 ECTS* in mandatory taught modules, with each degree-awarding institution contributing one 5-ECTS module;
  - *15 ECTS* allocated to the Master's thesis.
- **30 ECTS – Elective Components:**
  - *15 ECTS* in elective modules aligned with a selected professional profile (with up to 10 recommended modules available per profile), supporting optional career specialisation;
  - *15 ECTS* in freely chosen elective modules, allowing for individual academic and professional development.

Students are strongly encouraged to select a professional profile and complete their electives accordingly. However, this is not mandatory. Learners may alternatively complete all 30 ECTS of elective study through freely chosen modules.

Teaching formats include online lectures, seminars, tutorials, exercises, project work, portfolios, and simulations. The specific learning and teaching methods for each module are described in the *Module Handbook* (Annex 7).

4.2 Programme Learning Outcomes

Graduates are expected to have achieved the overarching learning goals listed in Table 5. These Programme Learning Outcomes (PLOs) were developed in line with the European Qualifications Framework (EQF) at Level 7 (Master's), international benchmarks, as well as stakeholder input from industry and academia.

Table 5: Overarching Learning Goals across the Joint Degree Program

No.	Programme Learning Outcomes
PLO1	Critically assess and evaluate cybersecurity principles, practices, and technologies relevant to modern enterprises.
PLO2	Strategically apply cybersecurity knowledge and utilise practical skills and technologies for long-term success in cybersecurity leadership roles across diverse industries, government agencies, and institutional settings.
PLO3	Identify knowledge gaps and undertake self-learning to acquire new knowledge to support professional development and the ability to adapt to evolving threats, technologies, and regulatory environments.
PLO4	Exhibit and apply leadership skills necessary for effectively managing cybersecurity initiatives within organisations, including education and training, strategic planning, and resource allocation.
PLO5	Critically evaluate and analyse cyber threats in order to implement effective security operations, and to enable the proactive identification, assessment, and mitigation of cyber threats.
PLO6	Effectively apply analytical and strategic thinking in order to make decisions to address security requirements.
PLO7	Communicate effectively across a range of complex and advanced cybersecurity concepts to provide leadership within an organisation and facilitate effective collaboration and teamwork.
PLO8	Critically assess cybersecurity legal, information governance, and regulatory frameworks and practices to ensure effective oversight, auditing, risk mitigation, accountability, compliance, and strategic alignment with organisational objectives.

4.3 Modules

Table 6 provides an overview of the modules that comprise the Online Master's Programme, including details on the delivering and accountable partner institutions.

For each module, one of the degree-awarding institutions is designated as the accountable institution: the Module Guarantor. This university assumes full academic and operational responsibility for the module, regardless of whether teaching is delivered by another higher education partner within the Digital4Security network.

The responsibilities of the Module Guarantor institution include:

- Ensuring the module aligns with programme-level learning outcomes;
- Ensuring the module content is suited for conveying the module-level learning outcomes;
- Reviewing and approving learning materials and assessments;
- Monitoring instructional quality and delivery;
- Serving as an additional point of contact for academic and administrative matters related to the module;
- Providing backup teaching capacity in case the delivering partner becomes unavailable or cannot fulfil their responsibilities.

The overview presented in Table 6 also includes information on modules recommended for different professional pathways, with the following abbreviations used:

- Chief Information Security Officer: CISO
- Cybersecurity Educator: Educator
- Cyber Legal, Policy, and Compliance Officer: Cyber Legal
- Cybersecurity Risk Manager: Risk Manager
- Cyber Threat Intelligence Specialist: Threat Intelligence
- Cybersecurity Auditor: Auditor.

Table 6: Overview of Modules, ECTS, Curriculum Relation and Partner Contributions

No.	Module	ECTS	Programme Relation	Delivering Partner	Module Guarantor
1	Communication Design for Cybersecurity	5	Mandatory	UDS	UDS
2	Business Resilience, Incident Management & Threat Response	5	Mandatory	MTU	MTU
3	Ethical Hacking & Penetration Testing	5	Mandatory	UNIR	UNIR
4	AI & Emerging Topics in Cybersecurity	5	Elective - recommended for CISO, Educator, Cyber Legal, Risk Manager	UDS	UDS
5	Malware Analysis	5	Elective - recommended for Threat Intelligence	UNIR	UNIR
6	Cybersecurity Culture, Strategy & Leadership	5	Elective - recommended for CISO, Educator	VMU/ ATAYA	UDS
7	Enterprise Architecture, Infrastructure Design and Cloud Computing	5	Elective - recommended for Threat Intelligence	UPB	MTU
8	Law, Compliance, Governance, Policy, and Ethics	5	Elective - recommended for CISO, Educator, Cyber Legal, Risk Manager, Auditor	UNIBS	MTU
9	Research Methods	5	Elective - recommended for Educator	UNI KO	UDS
10	Security Operations	5	Elective - recommended for Risk Manager, Threat Intelligence, Auditor	CY CERGY	UNIR
11	Technological Foundations for CS & Security Controls	5	Elective - recommended for Risk Manager, Threat Intelligence	UPB	UNIR
12	Automation of Security Tasks and Data Analytics	5	Elective - recommended for Threat Intelligence	UNIRI	UNIR
13	CISO and Crisis Communication	5	Elective - recommended for CISO	VMU/ ATAYA	UDS
14	Risk Management of Cyber-Physical Systems	5	Elective - recommended for CISO, Risk Manager, Auditor	POLIMI/ CEFRIEL	MTU

No.	Module	ECTS	Programme Relation	Delivering Partner	Module Guarantor
15	Cybersecurity Auditing	5	Elective - recommended for Cyber Legal, Auditor	VMU/ ATAYA	UNIR
16	Cybersecurity Economics & Supply Chain	5	Elective - recommended for CISO, Risk Manager	MRU	UDS
17	Cybersecurity Education & Training Delivery I	5	Elective - recommended for Educator	BUT	UDS
18	Cybersecurity Education & Training Delivery II	5	Elective - recommended for Educator	UPB	UDS
19	Cybersecurity in Industry - Security of OT & CPS	5	Free Elective	POLIMI	MTU
20	Cybersecurity Law & Data Sovereignty	5	Elective - recommended for Cyber Legal, Auditor	BUT	MTU
21	Machine and Deep Learning in Cybersecurity	5	Free Elective	UNIRI	UNIR
22	Digital Forensics, Chain of Custody and eDiscovery	5	Elective - recommended for Cyber Legal, Auditor	UPB	UNIR
23	Threat Intelligence	5	Elective - recommended for Threat Intelligence	UPB	UNIR
24	Thesis	15	Mandatory	UNI KO	UDS

To ensure that all graduates have undertaken academic work at each of the three awarding institutions, the programme requires students to complete one mandatory module at each partner university. This structure guarantees that every student has genuinely studied at all institutions jointly conferring the degree.

The mandatory modules are designed to provide complementary core perspectives aligned with the programme's overarching focus on Cybersecurity Management and Data Sovereignty, particularly in the context of Small and Medium-sized Enterprises (SMEs). Specifically:

- At the German University of Digital Science (UDS), a module develops managerial competence through communication and strategic design skills;

- At Munster Technological University (MTU), a business-oriented module focuses on organisational resilience;
- At Universidad Internacional de La Rioja (UNIR), a technically oriented module deepens knowledge in cybersecurity operations.

Together, these modules ensure that every student gains foundational knowledge across the programme's three essential pillars: management, business, and technology – in the context of cybersecurity and data sovereignty.

In addition, the Master's Thesis module, worth 15 ECTS, is a mandatory component in which students are expected to apply and demonstrate their competencies across the full range of Programme Learning Outcomes, integrating knowledge, skills and competencies acquired throughout their studies.

Beyond the limited number of formally mandatory modules, the programme includes various non-mandatory components. Elective modules may be chosen freely or selected from predefined sets aligned with specific professional profiles (see Section 4.5).

The curriculum modules are mapped to the Programme Learning Outcomes (PLOs) as outlined in Table 7. Both the module content and the associated assessments must be designed to effectively support the PLOs to which the respective module is assigned. This alignment is regularly re-evaluated using, at a minimum, the dedicated instruments defined in the *Programme Survey Scales* (Annex 5).

Table 7: Overview of Each Module's Contribution to the Programme's Learning Outcomes

No.	Module	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
1	*Communication Design for Cybersecurity*	X	X	X	X		X	X	X
2	*Business Resilience, Threat Response, and Incident Management*	X	X	X	X	X	X	X	X
3	*Ethical Hacking & Penetration Testing*	X	X	X		X	X		
4	*A.I. & Emerging Topics in CyberSecurity*	X	X	X		X	X		X

No.	Module	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
5	*Malware Analysis*	X	X			X	X		
6	*Cybersecurity Culture, Strategy & Leadership*	X	X	X	X		X		X
7	*Enterprise Architecture, Infrastructure Design and Cloud Computing*	X	X			X	X		
8	*Law, Compliance, Governance, Policy, and Ethics*	X	X		X		X		X
9	*Research Methods*	X	X	X		X	X	X	
10	*Security Operations*	X	X			X	X		
11	*Technological Foundations in Computer Science and Security Controls*	X	X			X	X		
12	*Automation of Security Tasks and Data Analytics*	X	X			X	X		X
13	*CISO and Crisis Communication*	X	X		X	X	X	X	
14	*Risk Management of Cyber-Physical Systems*	X	X			X	X		
15	*Cybersecurity Auditing*	X	X		X		X	X	X
16	*Cybersecurity Economics & Supply Chain*	X	X	X		X	X		X
17	*Cybersecurity Education and Training Delivery I*	X	X		X		X	X	
18	*Cybersecurity Education and Training Delivery II*	X	X		X	X	X	X	
19	*Cybersecurity in Industry – Security of OT and Cyber-Physical Systems*	X	X			X	X	X	X
20	*Cybersecurity Law & Data Sovereignty (BUT)*	X		X	X		X		X
21	*Machine and Deep Learning in Cybersecurity*	X	X			X	X		
22	*Digital Forensics, Chain of Custody and eDiscovery*	X	X			X	X	X	X
23	*Threat Intelligence*	X	X		X	X	X		X
24	*Thesis*	X	X	X	X	X	X	X	X

4.4 Module Descriptors

Each module is accompanied by a detailed descriptor, forming part of the *Module Handbook* (Annex 7). These descriptors specify:

- Module designation
- Contact details (name and/or email) of the delivering partner and the Module Guarantor institution
- Relation to the curriculum (mandatory / elective – may include recommendations for one or more professional profiles)
- Term of delivery (for mandatory modules)
- Teaching methods
- Workload (including contact hours and self-study hours)
- Credit points (ECTS)
- Prerequisites for joining the module
- Module summary
- Module learning outcomes
- Weekly content overview
- Examinations and assessment formats
- Reading list

The language of instruction and the examination requirements are not included in the individual module descriptors, as they apply uniformly across all modules and are specified centrally in the Module Handbook.

- The language of instruction is English.
- To pass a module, students must achieve at least 60% of the total available points.

The interpretation of performance levels is consistent across all modules and defined in Section 5 of the Study and Examination Regulations.

The Module *Handbook* specifies the term of delivery for mandatory modules only, as these are consistently scheduled to ensure a coherent learning progression across cohorts. For elective modules, the specific term of delivery is not fixed in the *Handbook*. Instead, the Master's Board determines which elective options are offered, and in which term, in full alignment with Section 4.6.

The list of elective modules available in a given academic year, including their respective term of delivery, is published at least one year in advance via the programme's online platform (where logically feasible – not for initial modules by the programme beginning), thereby enabling students to make informed and timely decisions in their study planning.

Mandatory modules may be offered more frequently than indicated in the Module Handbook, which specifies only the assured minimum frequency of delivery; additional instances may be scheduled to accommodate higher enrolment demand.

The Module Handbook is accessible to all students via the programme's learning platform and is regularly updated to reflect potential curricular enhancements. Core elements such as Intended Learning Outcomes and ECTS credits may only be adjusted through formal re-accreditation. Other supporting details may be adapted to facilitate continuous improvement, provided they remain fully aligned with the fixed elements of the curricular framework.

Further information on which curricular aspects may or may not be changed without re-accreditation is provided in the *Student Handbook* (Annex 8), in the context of fostering student engagement in programme development.

4.5 Professional Profiles

To support career orientation, students are encouraged to select a professional profile upon admission. Each profile corresponds to a recommended set of modules curated by a designated partner university, which provides academic leadership and targeted guidance. Students enrolled in a professional profile benefit from tailored academic support, as detailed in the *Student Handbook* (Annex 8).

Profile Overview and Curating Institutions:

- **Chief Information Security Officer (CISO)** – Focused on strategic leadership and management of an organisation's cybersecurity approach (curated by UDS).
- **Cybersecurity Educator** – Teaching and promoting cybersecurity awareness and best practices within organisations (curated by UDS).
- **Cyber Legal, Policy, and Compliance Officer** – Concentrating on the legal and regulatory aspects of cybersecurity, ensuring compliance with relevant laws and policies (curated by MTU).
- **Cybersecurity Risk Manager** – Dedicated to identifying, assessing, and mitigating risks to information security (curated by MTU).
- **Cyber Threat Intelligence Specialist** – Gathering and analysing threat intelligence to inform defensive strategies (curated by UNIR).
- **Cybersecurity Auditor** – Focused on evaluating and improving an organisation's cybersecurity policies, practices, and controls (curated by UNIR).

While professional profiles are not listed on the Degree Certificate – which uniformly confers the Master of Science – they are formally documented in the Diploma Supplement as evidence of career-specific preparation.

To receive formal recognition of a professional profile in the Diploma Supplement, students must complete at least 15 ECTS from the profile's recommended modules.

The terms and conditions for enrolling in a professional profile, as well as for switching between profiles, are specified in the *Student Handbook* (Annex 8).

Although it is possible to complete the Master's Programme without selecting a professional profile, this is not recommended. Students who choose not to follow a profile may freely select 30 ECTS of electives from the full range of available modules. However, students are strongly encouraged to indicate their intended profile at the time of admission to benefit from targeted academic and career guidance provided by the curating institution.

Overall, this approach is intended to provide maximum flexibility, while enabling students to structure their studies in a targeted manner, aligning with market-relevant and high-demand professional career pathways.

At a glance, the recommended modules per professional profile are as follows:

Chief Information Security Officer (CISO)

1. Cybersecurity Culture, Strategy & Leadership
2. Law, Compliance, Governance, Policy, and Ethics
3. Cybersecurity Economics & Supply Chain
4. Risk Management of Cyber-Physical Systems
5. CISO and Crisis Communication
6. AI & Emerging Topics in Cybersecurity

Cybersecurity Educator

1. Cybersecurity Education & Training Delivery I
2. Cybersecurity Education & Training Delivery II
3. Cybersecurity Culture, Strategy & Leadership
4. Research Methods
5. Law, Compliance, Governance, Policy, and Ethics
6. AI & Emerging Topics in Cybersecurity

Cyber Legal, Policy, and Compliance Officer

1. Law, Compliance, Governance, Policy, and Ethics
2. Cybersecurity Auditing
3. Cybersecurity Law and Data Sovereignty
4. AI & Emerging Topics in Cybersecurity
5. Digital Forensics, Chain of Custody and eDiscovery

Cybersecurity Risk Manager

.

1. Risk Management of Cyber-Physical Systems
2. Cybersecurity Economics & Supply Chain
3. Security Operations
4. Technological Foundations in CS & Security Controls
5. Law, Compliance, Governance, Policy, and Ethics
6. AI & Emerging Topics in Cybersecurity

Cyber Threat Intelligence Specialist

1. Threat Intelligence
2. Technological Foundations in CS & Security Controls
3. Security Operations
4. Automation of Security Tasks and Data Analytics
5. Malware Analysis
6. Enterprise Architecture, Infrastructure Design and Cloud Computing

Cybersecurity Auditor

.

1. Cybersecurity Auditing
2. Law, Compliance, Governance, Policy, and Ethics
3. Cybersecurity Law and Data Sovereignty
4. Risk Management of Cyber-Physical Systems
5. Security Operations
6. Digital Forensics, Chain of Custody and eDiscovery

4.6 Availability of Modules and Professional Profiles

The Joint Master's Programme in Cybersecurity Management and Data Sovereignty offers a diverse set of elective modules and curated professional profiles. While not all elective modules or profiles may be available at all times, students are ensured access to:

- The three mandatory taught modules (one from each awarding institution);
- The Thesis Module available across all three terms;
- A meaningful selection of elective modules sufficient to complete the programme successfully;
- The modules necessary to fulfil the requirements of any active professional profile, with at least four recommended modules from the profile made available within each academic year.

5. Grading System

The grading framework of the Joint Degree Programme is outlined in Table 8. It defines student performance in relation to the intended learning outcomes, based on the percentage of points achieved relative to the total points available.

This grading scheme is applied uniformly to both individual module assessments and the overall evaluation of programme performance.

The framework follows the principles of the European Credit Transfer and Accumulation System (ECTS), ensuring consistency and transparency in evaluating academic achievement.

Table 8: Joint Programme Grading Scheme

Points	Joint Label	Performance Level Description
90 – 100 %	**Excellent**	Performance is outstanding, significantly and consistently above the pass level
80 – 89 %	**Good**	Performance is strong, with many aspects exceeding the pass level
70 – 79 %	**Satisfactory**	Performance is fair, with some aspects exceeding the pass level
60 – 69 %	**Sufficient**	Meets all minimum intended learning outcomes
< 60%	**Fail**	Minimum intended learning outcomes are not achieved

5.1 Joint Grade Conversion Scheme

To ensure transparency and comparability across all partner institutions involved in the Joint Degree Programme, the following grade conversion table is applied (Table 9). It aligns the joint percentage grade, used consistently throughout the

programme, with the respective national grading schemes of Germany, Ireland, and Spain.

Table 9: Joint Grade Conversion Table

Points	Joint Label	German Grade	Irish Grade	Spanish Grade
90 – 100 %	**Excellent**	1 (sehr gut)	A (First Class Honours)	9–10 (sobresaliente)
80 – 89 %	**Good**	2 (gut)	B (Upper Second Class Honours)	7–8.9 (notable)
70 – 79 %	**Satisfactory**	3 (befriedigend)	C+ (Lower Second Class Honours)	6–6.9 (aprobado)
60 – 69 %	**Sufficient**	4 (ausreichend)	C– (Pass)	5–5.9 (aprobado)
< 60%	**Fail**	5 (mangelhaft / nicht bestanden)	F (Fail)	0–4.9 (suspenso)

This conversion scheme is jointly agreed upon by the partner institutions and is consistently used for the purposes of grade recognition and certification within the programme. National laws governing transcript formats or national awards may continue to apply in parallel.

Interesting to Know

Across the consortium, the pass thresholds of the individual institutions differ. In their own programmes, MTU applies a pass mark of 40%, UNIR a pass mark of 50%, and UDS a pass mark of 60%. For the Joint Degree Programme, the partner institutions have agreed to apply the most stringent threshold, namely the UDS pass mark of 60%, as the binding standard for passing. This pass mark applies to all students and across all participating institutions — UDS, MTU, and UNIR — within the Joint Programme. To ensure consistency and fairness, the finer grading distinctions above the pass level at MTU and UNIR have been mapped to the corresponding above-pass categories in the joint grading scale.

5.2 Mutual Recognition of Grades

All partner institutions mutually recognises grades awarded within the programme. No formal grade conversion is required for the purpose of awarding the Joint Master's Degree. The Joint Diploma Supplement will document:

- The percentage grade;
- The performance level description;
- National grade equivalents.

Where a grade must be interpreted by a national authority or employer, Table 9 shall serve as the official reference.

6. Assessment, Proctoring, and Scalability

The Master's Programme in Cybersecurity Management and Data Sovereignty ensures full alignment of all assessment and grading regulations and practices with the European Approach for Quality Assurance of Joint Programmes. This serves to guarantee fairness, transparency, and academic integrity in all assessment procedures, irrespective of delivery format or national context.

Given the programme's fully online format, its strategic objective to support Small and Medium-sized Enterprises (SMEs) in strengthening European cybersecurity, and its ambition to serve several thousand concurrently enrolled students, assessment strategies are designed to combine the following key principles:

- Rigorous verification of individual achievement,
- Authentic and relevant tasks aligned with professional practice,
- Scalable and sustainable implementation methods.

The regulations outlined in this manual are designed to ensure consistency in grading practices and to promote the equitable measurement of learning outcomes across all partner institutions. Further practical guidance on assessment design is available to teaching staff in the *Practical Guide for Lecturers* (Annex 10).

All assessment design within the programme should support both formative and summative learning, while reflecting the diversity of learner backgrounds and enabling students to integrate their own professional experience and career goals into their academic work. Formative assessments are designed to provide ongoing feedback that supports learning and improvement, while summative assessments evaluate student performance at the end of a module against defined learning outcomes.

6.1 Module Guarantor Procedure

To ensure both academic excellence and pedagogical responsiveness, instructors delivering a module are entitled and expected to propose the assessment and proctoring formats, prioritizing those that best align with the intended learning outcomes and the module's subject matter.

In cases where a module is delivered by an associate partner institution within the Digital4Security network, the design of the assessments is led by that institution. However, final grade assignment and quality assurance remain the responsibility of the module's accountable partner institution, the Module Guarantor, which is one of the three degree-awarding universities: UDS, MTU, or UNIR.

In determining the module's most appropriate proctoring method, each instructor from the associate institution shall ensure that:

- The approach reliably verifies the student's identity and authorship.
- All expectations, restrictions, and procedures can be clearly communicated to students at the beginning of the module.
- The approach complies with the overarching academic integrity and scalability principles of the programme.

To ensure consistency across the programme, associate partner institutions must submit the following documentation to the accountable partner institution at least one month prior to the start of the teaching term:

- A detailed outline of the assessment design (e.g. quizzes, assignments, group projects);
- A description of the proctoring or identity verification procedures proposed for the minimum 60% of proctored assessment contributing to the final module grade;
- Access to all teaching materials associated with the module;
- Where applicable, a list of any revisions made since the module was last delivered.

The Module Guarantor institution evaluates the submitted materials in accordance with procedure QAP.05 of the *Internal Quality Handbook* (Annex 4), utilizing the evaluation tools provided in the *Programme Survey Scales* (Annex 5).

If no changes have been made to the module since its last offering, the Guarantor institution may confirm its previous assessment.

The outcome of the module review shall be submitted to **quality.committee@digital4security.eu** no later than two weeks after the start of the term in which the module is delivered.

The Master's Board of Directors is responsible for:

- Recommending standardised assessment and proctoring procedures that ensure cross-institutional consistency and compliance.
- Supporting the programme by identifying or providing access to reliable platforms and tools (e.g., proctoring software, grading interfaces) for assessment delivery and monitoring.

This shared governance model allows each module to benefit from local pedagogical expertise while upholding the shared standards and legal responsibilities required in a Joint European Master's Programme.

Tools such as the following are recommended for core assessment-related functions:

- **Proctoring:** *SMOWL* or similar tools and services are recommended for remote exam proctoring.
- **Plagiarism Detection:** *Turnitin* or similar tools and services are recommended for checking academic integrity in written submissions.

6.2 Assessment Transparency

All assessments must be transparently documented in advance via the programme's Learning Management System (LMS). This documentation must include, where applicable:

- Assessment schedules and grade weightings;
- Proctoring procedures and tools;
- Grading rubrics;
- Peer review rubrics (if peer assessment is used).

6.3 Assessment Weighting and Proctoring Requirements

Each module must assign a minimum of 60% of the final grade to verified or proctored assessment, and up to 40% to continuous assessment. This 60–40 model provides the dual benefit of:

- Securing the academic integrity and verifiability of core assessments, and
- Allowing flexibility for creative, reflective, and practice-oriented learning.

6.3.1 Proctored Assessment (≥60%)

Proctored assessment ensures that a student's identity is confirmed, and that the submitted work was produced independently and ethically, using only permitted tools and sources. Proctoring may take multiple forms, depending on the nature of the module and the type of assessment involved.

Permitted forms of proctored assessment include:

- Online exams using a GDPR-compliant digital proctoring tool, such as SMOWL (which is already in standardised use at UDS and UNIR, the two fully-online universities within the consortium).
- Live oral presentations or defences conducted synchronously with identity verification.
- Employer-verified projects, where an industry partner, supervisor, or professional mentor attests that the student has completed the work independently (for further details on the procedure, see section. 7.7).

Where proctoring technology such as SMOWL is used, any detected anomalies (e.g. use of unauthorised materials, second-person presence, or suspicious background activity) are flagged to the instructor for review. Confirmed violations of proctoring rules will lead to failure of the proctored assessment component.

6.3.2 Continuous Assessment (≤40%)

The remaining portion of the module grade, up to 40%, may be awarded through continuous assessment, designed to maintain engagement, support learning progression, and foster independent thinking. These activities are integrated into the Learning Management System (LMS) and may include:

- Weekly learning tasks (e.g. short responses, guided exercises, simulations),
- Case-based analyses
- Problem-solving or design tasks,
- Online discussions,
- Reflection logs or portfolios,
- Automated quizzes with immediate feedback.

To further personalise the learning journey and recognise prior knowledge, instructors are encouraged to:

- Offer alternative but equivalent task formats, allowing students to choose between assignments of similar difficulty but different focus (e.g. legal, managerial, technical),
- Include bonus-point opportunities that reward in-depth exploration,
- Enable students to integrate their professional context into submissions, e.g. by applying theory to their own organisational setting.

Where feasible, adaptive or automated tools can be used to support formative feedback without increasing the workload of instructors. This includes self-graded quizzes, rubrics for peer feedback, and conditional content pathways.

Instructors are expected to provide timely and constructive feedback throughout the module, which may take different forms, such as:

- Feedback discussions in a live session,
- Written comments,
- Annotated submissions,
- Recorded voice or screen feedback,
- Peer input guided by clear rubrics,
- Instructor-prepared automated feedback, e.g., in the context of quizzes.

The objective of continuous assessment is not only to measure progress, but to support autonomous, confident learners capable of reflecting critically and acting ethically in professional settings.

6.4 Resits and Repeat Assessments

Learning is a dynamic process, and occasional challenges are recognised as part of meaningful academic and professional development. To support student success and uphold the integrity of the qualification, the programme provides clearly defined opportunities to re-sit examinations and repeat assessments. These measures are designed to enable students to demonstrate mastery of the intended learning outcomes, while maintaining fairness and upholding the jointly agreed high academic standards across all awarding institutions.

6.4.1 Examination Opportunities per Module Enrolment

Modules that include a final examination component offer two scheduled examination sessions per enrolment:

- **Ordinary Call**: This constitutes the primary examination session, typically held at the conclusion of the teaching period for the module. All students are expected to undertake the final examination during this session.

- **Extraordinary Call**: This serves as a second and final opportunity to undertake the examination within the same enrolment period. It is available only to students who (a) did not achieve a passing grade in the Ordinary Call, or (b) were unable to attend the Ordinary Call. If no students qualify under these conditions, the Extraordinary Call is cancelled.

Dates for the Ordinary and Extraordinary Calls are published in advance and communicated to students at the beginning of the term, in accordance with Section 6.2, and in line with the academic calendar requirements specified in Section 2.

The scope and format of the Extraordinary Call will generally mirror those of the Ordinary Call. The *Module Handbook* (Annex 7) may offer additional information on module-specific assessment and reassessment formats.

6.4.2 Module Re-Enrolment

Students are permitted a maximum of two examination attempts per module enrolment: one in the Ordinary Call and one in the Extraordinary Call.

If a student does not successfully complete the module after both opportunities, they may re-enrol in the module in a subsequent academic term. Re-enrolment requires the student to complete all components of the module anew. This includes, but is not limited to:

- Resubmission of all required coursework and assignments;
- Participation in all formative and summative assessments;
- Completion of the final examination, where applicable.

No grades or partial results from previous enrolments are carried forward. Each enrolment constitutes a new and independent opportunity to fulfil the module's intended learning outcomes.

6.4.3 Maximum Number of Examination Attempts

No single examination may be attempted more than four times in total, including all attempts made across repeated module enrolments. Students are strongly advised to monitor their number of attempts, particularly in mandatory modules, which must be successfully completed in order to obtain the Master's Degree.

If a student fails to pass the examination in a mandatory module after four attempts, they will no longer be eligible to complete the programme. However, a Transcript of Records will be issued, documenting all successfully completed modules and corresponding grades. In line with microcredential and lifelong learning frameworks, these may serve as formal recognition of the competencies acquired, even where the full degree is not awarded.

6.5 Late Submission of Coursework

Meeting published deadlines for assignments and assessments is essential to ensuring fairness for all students and maintaining the smooth progression of the programme. Timely submission also supports the development of effective time management skills, which are vital for professional success. All coursework and assessment components are therefore expected to be submitted by the deadlines communicated in the respective module schedules.

6.5.1 Exceptional Circumstances

In cases of exceptional and well-documented circumstances, students may request an extension or alternative assessment arrangement. Valid reasons for late submission may include, but are not limited to:

- Serious illness or scheduled medical procedures (e.g., surgery);
- Bereavement (e.g., the loss of a close family member);
- Natural disasters or major emergencies directly affecting the student's ability to study or submit work;
- Other significant, unforeseen events beyond the student's control.

Requests must be submitted as early as possible and supported by appropriate documentation (e.g., medical certificate, official notice of emergency).

6.5.2 Procedure for Requesting Late Submission

Students must take the following steps when seeking an extension due to exceptional circumstances:

- **For a single module**: Contact the relevant course instructor directly. With valid documentation, the instructor may grant a short extension or propose an alternative assessment arrangement at their discretion.

- **For multiple modules**: If the issue affects the student's ability to engage with several modules (e.g., due to a natural catastrophe or medical emergency), the student shall contact their Programme Coordinator, copying all relevant instructors in the communication.
- **For general academic challenges**: If the student is falling behind more broadly (e.g., across multiple modules, due to time management issues or personal circumstances), they should contact **studyaffairs@digital4security.eu**. The team can assist in identifying suitable support measures, including potential changes to the study track (e.g., from full-time to part-time) or the withdrawal from individual modules.

6.5.3 Unacceptable Grounds for Late Submission

The following are not considered valid grounds for late submission:

- Conflicting work obligations or deadlines;
- Travel or holiday plans;
- General workload or time pressure without exceptional cause.

Students are expected to manage their time effectively and to seek assistance early if they encounter difficulties.

6.6 External Evaluation: Ensuring Shared Standards across Europe

As a joint European Master's degree, this programme benefits from the diverse academic and professional perspectives contributed by the three awarding universities and the wider Digital4Security partner network. To ensure consistency, transparency, and fairness in the evaluation of student performance, external and cross-institutional evaluation mechanisms are applied.

- External examiners and cross-institutional reviewers may be appointed to evaluate selected assessments. These may include, but are not limited to, master's theses and module assessments, including proctored examinations.
- All evaluations are conducted in accordance with shared rubrics, and transparent assessment criteria are followed as agreed across the partner institutions.
- Final marks are determined either by averaging scores across reviewers or by consensus, depending on the nature of the assessment.

This approach supports the harmonisation of academic standards across institutions, reinforces the integrity of joint academic awards, and ensures alignment with international best practices in higher education assessment.

The Examinations Board retains the authority to define reviewer and examiner requirements for each type of evaluation. This includes, where applicable, confirming the eligibility and appointment of thesis supervisors, external examiners, and second markers in line with institutional regulations and programme-wide quality assurance standards.

6.7 Scalable Assessment Formats

To ensure academic excellence and efficient delivery across large and diverse student cohorts, the programme encourages the use of scalable assessment formats. These methods not only reduce grading workload, but also foster collaborative learning and critical reflection: key competencies for cybersecurity professionals.

Two approaches are especially recommended:

- Team-Based Assignments
- Peer Assessment

Overall, scalable formats are central to maintaining pedagogical quality and efficiency as the programme grows to accommodate thousands of learners. By blending teamwork, reflection, and peer evaluation, instructors can foster meaningful learning experiences while managing assessment volume sustainably.

Further recommendations for online assessment can be found in the *Practical Guide for Lecturers* (Annex 10), forming part of the Joint Programme Documents, and in the Scientific Report *Assessment Methods for Scalable Online Programmes: State of the Art and Future Directions* by UDS.

6.8 Appealing Assessment Outcomes

6.8.1 Grading Appeals

Students wishing to contest a grade should first submit an informal request for an assessment review session with the responsible examiner within one week of the grade being issued. The review session should then take place within one week of the student's request. This session provides an opportunity for students to discuss the evaluation and seek clarification. The examiner may convene a joint review session for all students in the module and is not obliged to accommodate individual scheduling requests, though individual meetings may be offered at the examiner's discretion.

If concerns remain unresolved after the review session, students may submit a formal grade appeal within three weeks from the issuance of the original grade. Appeals are first addressed at the institutional level, with the procedure detailed in the *Student Handbook* (Annex 8).

Should the matter remain unresolved at the institutional level, the appeal may be escalated to the Examinations Board. The Master's Board of Directors serves as the final authority for appeal resolution.

For confidential advice or in case of uncertainty regarding the appeals process, students may contact the ombudsperson at **ombudsperson@digital4security.eu**.

6.8.2 Peer Review Appeals

If a student believes that their peer review assessment was unfair, the following procedure applies:

- The student may submit a written request to the course instructor within one week of the peer grading publication, including an explanation of their concern. This may be done, for example, via Moodle's feedback or messaging system.
- The instructor will review the submission and the relevant peer evaluation within one week.
- If the concern is substantiated, the grade will be manually adjusted.
- Should the student remain dissatisfied after this review, the instructor-confirmed grade shall be considered the official grade issuance date. The student may then request an informal grade review session with the instructor within one week of this date, following the procedure outlined in Section 6.8.1.

7. Thesis Module

The Thesis Module is a mandatory component of the Joint Master's Degree Programme and is worth 15 ECTS credits. It represents the culmination of the student's academic journey through the programme, requiring the demonstration of advanced competencies in the fields of Cybersecurity Management and Data Sovereignty.

The module consists of two components:

- A written thesis;
- An oral defense.

7.1 Purpose

The Master's thesis serves to demonstrate the student's ability to conduct independent, critical, and methodologically sound research or applied project work in the field of Cybersecurity Management and Data Sovereignty. In completing the thesis, students are expected to:

- Identify and articulate a relevant and complex problem;
- Select and apply appropriate research and/or design methodologies;
- Critically engage with current academic and professional literature;
- Develop viable solutions or well-founded recommendations suitable for real-world cybersecurity contexts;
- Critically evaluate the developed solution, outlining its benefits and limitations in a substantiated manner;
- Communicate findings clearly and effectively in both written and oral formats;
- Demonstrate autonomy in project management by completing the thesis independently and within the established timeframe.

7.2 Work-Integrated Projects

To foster authentic, high-impact learning and to support the students' transition into professional roles, the programme offers structured opportunities for students to undertake a work-based research project in collaboration with industry or public sector partners. These projects form an integral component of the Digital4Security initiative and are designed to promote fruitful exchange between academic insight and practical cybersecurity challenges.

Work-based thesis projects are embedded in the operational contexts of participating companies, institutions, or cybersecurity networks. Students apply their acquired knowledge to concrete challenges, contributing to the co-creation of innovative solutions while being jointly supervised by an academic advisor and a professional mentor. This dual supervision ensures both scientific quality and real-world relevance.

7.2.1 Project Proposals

Each project proposal must undergo formal approval by the Examinations Board. The Board may delegate this responsibility to one or more of its members, who are authorised to review and accept proposals on the Board's behalf. Approval is contingent upon the academic suitability of the proposed work and its feasibility within the duration of the thesis.

Two primary modes of project initiation are foreseen:

1. **Organisation-initiated proposals**: Participating organisations (such as SMEs, corporate partners, or public bodies) may submit project offers. This mode is particularly suitable when an organisation identifies a practical challenge, such as the redesign of a cybersecurity incident response strategy, and seeks a qualified student to address it.

2. **Joint student-organisation proposals**: In cases where students and organisations already collaborate (for instance, when a student is employed as a working professional) joint proposals may be submitted for a specific topic and pairing. This option is well-suited to students who are already working and who wish to address a problem they have encountered in their professional context.

For proposals initiated by organisations, the following information must be provided:

- Project title;
- A concise profile of the hosting organisation;
- Description of the cybersecurity management and/or data sovereignty challenge to be addressed;
- Desired qualifications or competencies of the student;
- Information on remuneration (optional);
- Name, position, and contact details of the proposed professional mentor;
- A draft of the proposed Learning Agreement, completing the programme's standard template;
- A statement confirming that the student will receive sufficient support and regular access to resources required for timely completion of the thesis.

In the case of joint student-organisation proposals, the desired qualifications or competencies of the student need not be specified. Instead, the following additional details are required:

- Full name and contact details of the student;
- Nature of the student's relationship to the organisation (e.g. employee, founder, intern);
- Brief statement on the duration and context of the student's affiliation with the organisation.

The Examinations Board is responsible for providing the standard Learning Agreement template, which must be adapted to each individual project. This agreement

shall be signed by the student, a representative of the hosting organisation, and an authorised representative of the Examinations Board. The agreement defines the project scope, delineates roles and responsibilities, and addresses data protection obligations and intellectual property rights. Projects involving sensitive or classified data must confirm compliance with relevant national and EU-level data security regulations. Any requirements regarding the intended Work Attestation (Section 7.7), which the student must obtain by the end of the project, need to be duly considered and reflected in the Learning Agreement at the start of the project.

7.2.2 Time of Proposal Submission

Work-Based Research Projects may be proposed at any time during the academic year by submitting the required documentation to the Examinations Board via **Examinations.Board@Digital4Security.eu**. The Examinations Board shall review submitted proposals within a period of four weeks (excluding term breaks). The Board may request further information or refinements before authorisation is granted.

To ensure the timely commencement of thesis work, it is strongly recommended that proposals jointly submitted by students and organisations be made well in advance of the thesis term. This allows sufficient time for academic review and the finalisation of the Learning Agreement, thereby supporting a seamless start to the thesis writing phase.

7.2.3 Proposal Reviews

In reviewing project proposals, the Examinations Board must ensure that the project will enable the student to fulfil the purpose of thesis-writing, as defined in Section 7.1. Furthermore, the Board must ensure that the project allows for sufficiently independent academic work, such that the unique contribution of the student can be clearly isolated and evaluated. The student's success shall not depend, to a notable degree, on the performance of other individuals within the hosting organisation or on the organisation's success as a whole.

In addition, the proposed Learning Agreement must be free of any non-disclosure provisions that would prevent the student from granting the thesis examination committee full access to all relevant data. It must be ensured that the student's approach to data processing and analysis is fully transparent and accessible to the academic evaluators, in accordance with the academic standards and integrity principles governing the assessment process.

7.2.4 Publication and Documentation

Accepted organisation-initiated project proposals are published on the learning platform. In addition, the programme may organise pitching events designed to facilitate match-making between organisations and students. To further support collaboration, interactive forums may be established to enable informal exchange between students and the wider programme network, including members of the Industry Advisory Board and representatives of participating institutions. These platforms may be used to share project proposals, post opportunities, submit expressions of interest or post search queries.

By contrast, documentation concerning approved student-organisation projects is routinely maintained by the Examinations Board and the Secretariat, as such projects are already assigned and do not require further match-making.

7.3 Thesis Supervision

Each student is entitled to guidance from at least one academic supervisor throughout the research, project execution, and thesis writing process. The supervisor must hold a professorial qualification (e.g., Professor or Junior Professor) or an equivalent rank recognised by their home institution, and possess a PhD (or equivalent doctorate) in a discipline relevant to Cybersecurity Management and Data Sovereignty.

Upon enrolling in the Thesis Module, students receive weekly support from the module instructor, focusing on general topics such as research organisation, time management, and writing strategies. This instructor may not be an expert in the student's specific thesis domain. Therefore, a second, subject-specific supervisor may be appointed to offer targeted guidance, and to serve as one of the examiners during the final evaluation.

Eligible supervisors for the programme shall be confirmed by the Examinations Board. The Board may maintain a list of approved supervisors, including their specific areas of expertise and their supervisory capacity (such as the number of students they are able to supervise per term).

Additionally, students may be supported by an informal thesis mentor, particularly in work-integrated projects. Mentors offer practical input, but do not participate in formal assessments.

Supervisors overseeing a work-based thesis project must ensure that a signed Learning Agreement is in place by the official start of the thesis writing phase. This agreement must include the signatures of the student, the hosting organisation, and the authorised representative of the Examinations Board. Where uncertainties arise, supervisors shall liaise with the Examinations Board to resolve any issues.

While students' preferences to explore particular domains within Cybersecurity Management and Data Sovereignty are to be supported wherever possible, it is the joint responsibility of the supervisor and the Examinations Board to protect students from structural risks that may hinder their academic performance or the timely completion of their thesis. For example, if a student undertakes thesis research for a work-based project before a Learning Agreement has been finalised, and the hosting organisation later imposes non-disclosure conditions that obstruct transparent academic evaluation, the student may be forced to change the thesis topic mid-term. Such scenarios must be proactively prevented.

In cases where students wish to pursue a thesis topic that is not directly work-based, supervisors confirmed by the Examinations Board are authorized to approve thesis topics. Supervisors are encouraged to approve topics generously, allowing students to explore preferred subjects within the scope of Cybersecurity Management and Data Sovereignty. At the same time, supervisors shall provide guidance to help students refine their topics to maximize the potential for strong academic performance.

In refining the thesis topic, supervisors and students should consider criteria such as the following:

- The topic should be appropriately scoped: not so narrow as to be insignificant, and not so broad as to exceed the allotted thesis writing period;
- The student must possess the necessary foundational knowledge to successfully engage with the topic;
- Required infrastructure and resources, including any associated costs, must be accessible and manageable;
- There should be sufficient existing literature to enable the required review of related works, while the problem addressed remains open and unsolved, offering genuine research value.

7.4 Duration

Formal registration for the Master's thesis occurs via enrolment in the Thesis Module. To be eligible, students must have successfully completed at least two mandatory taught modules and accumulated a minimum of 30 ECTS credits.

The thesis duration depends on the study track:

- One academic term for full-time or accelerated part-time students;
- Two academic terms for regular part-time students.

A grace period of up to two additional weeks is permitted for the thesis submission beyond the official thesis duration.

The thesis defence must take place no later than eight weeks into the following academic term after the official thesis period ends.

Each student may request one extension, granting one additional term for completing the thesis. The first request is accepted automatically if submitted during the active term to: **Secretariat@digital4security.eu**.

Further extensions require formal justification (e.g., a certified medical condition). If at least six weeks of reduced working capacity are documented during the original thesis period, the Secretariat may grant a second extension automatically. All other cases must be reviewed and decided by the Examinations Board.

7.5 Submission

The standard thesis format, including detailed requirements such as length, structure, and mandatory components, will be provided and explained at the start of the Thesis Module.

The thesis must be submitted via the designated submission portal on the learning platform and must include:

- The final thesis in PDF format, encompassing:
  - A plagiarism declaration, hand-signed or electronically signed by the student, confirming that the work is the student's own and that all sources have been properly acknowledged;
  - In the case of work-integrated projects, a supporting attestation from the employer or mentor (see Section 7.7), included in the annex.

7.6 Template

To ensure consistency, academic rigour, and alignment with the programme learning outcomes, all Master's theses must adhere to standardized formatting and structural guidelines. The official thesis template is made transparently available to all students on the learning platform. Detailed instructions on working with the template are provided to students enrolled in the Thesis Module, where they receive step-by-step guidance throughout the thesis writing process.

The thesis template must be authorized by the Master's Board. The template shall be reviewed at least annually to reflect evolving academic standards and programme requirements.

The thesis submission must include the following essential components:

- **Title Page:** Includes thesis title, student name, student ID, supervisor(s), mentor(s), degree programme, and submission date.
- **Attestation:** Hand-signed confirmation by the student that the work is their own, produced independently, and using only permitted resources transparently documented within the thesis.
- **Abstract:** A concise summary highlighting the identified problem, methodological approach, key findings, proposed solution or recommendations, and an evaluation of the thesis' contribution to the field.
- **Table of Contents:** Listing chapters, sections, and corresponding page numbers.
- **Introduction and Problem Statement:** Clear articulation of a relevant and complex cybersecurity management and/or data sovereignty problem, including its context and significance.
- **Literature Review and Analysis:** A critical engagement with current academic and professional literature to establish the theoretical and practical foundation of the work. This includes a thorough review of existing approaches and solutions, accompanied by a clear discussion or evidence demonstrating why the specific problem addressed in the thesis remains inadequately solved by already existing methods.

- **Methodology:** Detailed explanation of the selected research and/or design methodologies, with justification of their appropriateness for addressing the problem.
- **Results / Solution:** Development and presentation of a viable solution, and/or actionable recommendations, tailored to real-world cybersecurity contexts. This section must include relevant data to evaluate the solution's performance in relation to the problem outlined in the introduction.
- **Critical Assessment:** Discussion of strengths and limitations of the thesis; implications for practice; recommendations for further research.
- **Conclusion:** Summary of key insights, and reflection on the thesis' overall contribution to the field.
- **References:** Complete, accurate, and consistently formatted list of all cited sources according to the prescribed citation style.
- **Appendices (if applicable):** Supplementary materials such as data sets, research instruments, or detailed calculations. For work-integrated projects, the workplace-attestation shall be included in the appendix (cf. Sect. 7.7).

The approved citation style (e.g., APA, IEEE, Chicago) shall be specified in the thesis template and must be applied consistently throughout the document.

7.7 Workplace Attestation

In cases where the thesis – or a proctored module assessment – is based on a work-integrated project, the student must submit an attestation from their workplace confirming:

- That the project was carried out independently by the student;
- That the student upheld professional and ethical standards.

The attestation must be signed by a person with direct supervisory or oversight responsibility, who is not subordinate to the student and free from conflicts of

interest - for example, not a business partner, close personal associate, or someone under the student's authority (e.g., not an organization's employee if the student is the organization's CEO).

Eligible individuals include:

- A direct manager or supervisor at the student's organisation;
- An external consultant formally overseeing the project;
- A mentor from the Digital4Security consortium, including affiliated industry partners;
- A senior officer from the host organisation (e.g. compliance officer, department head);
- A university-appointed academic supervisor with direct insight into the project.

The person providing the attestation must explicitly declare their independence and absence of conflict of interest. The programme reserves the right to request clarification or a second attestation if concerns arise regarding the validity or impartiality of the submission.

This attestation must be included as an annex to the thesis. It forms part of the final thesis documentation.

7.8 Evaluation Criteria

The final thesis grade is determined on the basis of pre-defined rubrics and evaluation guidelines, established by the Examinations Board under the supervision of the Master's Board. The assessment considers aspects such as:

- Problem definition and relevance;
- Depth of research or technical application;
- Use of appropriate methodology;
- Quality of argumentation, analysis and presentation;

- Adherence to ethical standards.

Exact grading guidelines are confirmed periodically, published on the learning platform prior to the thesis term, and are binding for all assessors.

7.9 Defence, Evaluation Procedure, and Documentation

The thesis is defended before an examination panel of two qualified examiners from different partner institutions. Both must hold a PhD (or equivalent) in a relevant discipline to Cybersecurity Management and Data Sovereignty. The subject-specific supervisor serves as one examiner. The panel must receive the final thesis at least two weeks prior to the defence.

The supervisor conducts a standardised plagiarism check. A written confirmation of the procedure and its outcome must be submitted to the second examiner at latest by the oral defence date.

Assessment is based on:

- Written thesis (75% of final grade),
- Oral defence (25% of final grade).

The examiners may confer to discuss their assessments. Subsequently, each examiner independently grades both components and calculates a composite grade, applying the weighting of 75% for the written thesis and 25% for the oral defence. The final thesis grade is determined by averaging the two composite grades.

If the examiners' composite grades differ by two or more performance levels (e.g., Excellent vs Satisfactory), the case must be referred to the Examinations Board. The Board may request additional documentation and will issue a final decision within four weeks of any active term (excluding the term breaks).

The thesis supervisor is responsible for submitting the following documentation to **Secretariat@digital4security.eu** within one week after the oral defence, including:

8. Final thesis version,
9. The plagiarism check confirmation signed by the supervisor,
10. Evaluation forms from both examiners,
11. Final grade report.

8. Academic Integrity, and Support for Good Scholarly Practice

Academic integrity involves a commitment to honesty, fairness, responsibility, and respect in all academic activities. Students must produce and present their own work, duly acknowledge the contributions of others, and refrain from inappropriate conduct, such as:

Academic misconduct

- Plagiarism (using someone else's words, ideas, or work without proper acknowledgement)
- Fabrication (making up data, results, or information)
- Falsification (altering or misrepresenting existing data, results, or information)

General misconduct

- Discriminatory language (insults targeting ethnicity, gender, religion, disability, age etc.)
- Incitement to violence
- Criminal acts (such as hacking the learning platform or other unlawful activities)

Academic integrity ensures the credibility of assessment outcomes, the trustworthiness of qualifications, the maintenance of a fair and transparent learning environment across all partner institutions, and a safe and supportive setting for all participants.

8.1 Fostering Integrity and Empowering Students as Ethical Professionals

Academic integrity is a cornerstone of scholarly and professional life. In this programme, integrity is not enforced through suspicion, but cultivated through clarity,

support, and shared purpose. It is trusted that learners given the appropriate tools, expectations, and respect will rise to excellence in both method and mind-set.

8.1.1 Learning to Use Artificial Intelligence (AI) Tools Responsibly

Generative AI tools and code assistants are now integral to professional practice in cybersecurity, data management, and related fields. Students are encouraged to engage with these tools – not to avoid them –, but to do so critically, transparently, and within the ethical framework of their academic environment.

Instructors may define, for each assignment:

- Which forms of generative or assistive tools (e.g. language models, code generators, AI-enhanced editors) are permitted, not admissible, or may be encouraged or discouraged.
- What elements of the assignment must be produced without automation, to ensure skill demonstration.
- What kind of disclosure is expected, including logs, citations, or reflective documentation.
- Whether authorship clarification may be requested (e.g. during oral presentations or interviews). For instance, students may be asked to explain their submitted code as an indicator of authorship and understanding.

These expectations are always set by the instructor, not by abstract or generic programme rules. Students are responsible for adhering to the specific assignment criteria.

To support ethical and critical engagement with automated tools, students receive guidance on:

- Citing and acknowledging AI-generated contributions.
- Reflecting on tool usage in learning journals or appendices.
- Identifying how generated content was adapted, validated, or integrated.

These training materials can be found in the Welcome Module year-round.

8.1.2 Building Confidence in Original Work

Academic writing, research, and programming are not gatekeeping mechanisms; they are skills that can be learned, improved, and mastered. The programme is committed to developing students' confidence in producing work that is both intellectually rigorous and personally meaningful.

This includes learning to:

- Synthesize diverse sources into coherent arguments or artefacts.
- Accurately acknowledge the contributions of others, whether textual, visual, or code-based.
- Demonstrate clear authorship, reflection, and conceptual ownership.

To support this:

- Students have access to Turnitin plagiarism detection via Moodle or similar tools, and are encouraged – not penalised – for using it proactively.
- A self-paced onboarding tutorial on Academic Integrity and Referencing is available year-round in the Welcome Module.
- Referencing mistakes or citation gaps are treated as learning opportunities, unless there is clear evidence of intentional deception.

8.1.3 Collaborative Learning vs. Collusion: Clarifying Expectations

Collaboration is not only encouraged – it is essential in today's professional world. Study groups, team projects, and shared problem-solving mirror the realities of the cybersecurity field in applied contexts. However, transparency around authorship is key to maintaining fairness in assessments.

Guidelines:

- Instructors must clearly specify whether each task is to be completed individually or collaboratively.
- For group assignments, individual contributions must be identifiable, for instance by version-control logs, clearly defined roles, or individual reflection statements.
- Peer assessments must be based on clearly defined rubrics, and instructors are responsible for monitoring consistency and fairness.
- When in doubt, students are strongly encouraged to ask. Clear communication is preferable to assumptions or retrospective concerns.

8.2 Responsible Use of Digital Platforms and Resources

The Joint Master's Programme in Cybersecurity Management and Data Sovereignty provides access to a range of digital platforms, communication tools, and learning resources essential for teaching, collaboration, and assessment. These include the Learning Management System, video-conferencing facilities, digital libraries, and other network-based services maintained by the partner institutions. The responsible and lawful use of these resources is integral to maintaining academic integrity, safeguarding personal data, and fostering a constructive learning environment.

8.2.1 Digital Etiquette (Netiquette)

Active and constructive participation is encouraged in all learning contexts. In synchronous sessions, this may include enabling video when technically feasible, contributing to discussions via audio or chat, and sharing insights that enrich collective understanding. In asynchronous environments, contributions that are respectful, relevant, and considerate of diverse perspectives strengthen the learning experience for all participants.

8.2.2 Confidentiality of Assessment Materials and Individual Answers

Assessment materials are provided exclusively for the purpose of completing the relevant assignment or examination. These materials must not be copied, circulated, or shared in any form – whether physically or digitally – within or outside the programme.

Individual responses or completed assignments submitted for assessment are likewise confidential. Sharing one's own work or that of another participant, whether in part or in full, is strictly prohibited.

Any breach of these confidentiality requirements constitutes a serious violation of the programme's academic integrity regulations. Such actions compromise the fairness of the assessment process and erode mutual trust within the learning community.

The following exceptions apply:

- In team-based projects, assigned team members are expected to share relevant materials among themselves to collaboratively fulfil their joint tasks.
- In work-based projects, students may discuss their work with mentors and colleagues, provided that all parties adhere to the terms and conditions set out in the Learning Agreement.

- For extensive projects such as the thesis, regular review sessions and peer discussions are explicitly encouraged as an integral part of the process, provided that the thesis as a whole remains the independent work of the identified author. In cases of doubt, students are encouraged to acknowledge key contributions by others, for example in a footnote or the acknowledgements section. The Welcome Module supports students in learning how to appropriately reference not only formal published sources, but also informal communications, and how to acknowledge any significant guidance received.

8.2.3 Use of Learning Materials

Learning materials provided through the programme, such as lecture recordings and slides, are intended solely for use within the programme. These materials must not be reproduced, distributed, or shared outside the programme. Unauthorised dissemination of programme materials may constitute a breach of academic integrity as well as a violation of copyright law.

The same standard applies to peer review activities. In some modules, participants may be given access to the work of others for the purposes of feedback, collaborative evaluation, or formative learning. Such work remains the intellectual property of its author and is to be treated with strict confidentiality.

However, if peer-reviewed material contains clearly harmful or inappropriate content – such as discriminatory language, incitement to violence, malicious code, or other elements that may compromise the security or wellbeing of the learning community – such concerns may and should be brought to the attention of the instructor. In such cases, the message shall include relevant excerpts or references to support and clarify the concern.

8.2.4 System Security

Responsible engagement in the online learning environment also involves protecting account credentials, using secure connections, and complying with applicable

data protection legislation, including the General Data Protection Regulation (GDPR). Any activity that compromises the security and fairness of the learning environment, including unauthorised system access, distribution of harmful code, or disruption of learning activities, is incompatible with the programme's values. Responsible use of digital platforms and resources supports an environment where collaboration, integrity, and professionalism can thrive, enabling the development of skilled cybersecurity leaders prepared to meet the challenges of a complex digital society.

8.2 Handling Suspected Misconduct: A Transparent and Supportive Process

While rare, serious academic misconduct may occur. In such cases, the programme follows a fair, respectful process designed to protect both academic integrity and student rights.
Process Overview:

- The student will be notified of any concern and is offered the opportunity to respond within two weeks after notification.
- An initial review will be conducted by the Examinations Board, and, if necessary, escalated to the Master's Board of Directors.
- A Disciplinary Committee, including faculty from at least two awarding institutions, may be convened for complex cases.
- Sanctions shall be proportionate, and developmental whenever possible:
    - Constructive feedback or revised submission.
    - Grade adjustment or nullification.
    - Temporary suspension or, in the most serious or repeated cases, expulsion from the programme.

Disciplinary decisions issued by the Examinations Board, a Disciplinary Committee, or the Master's Board shall be communicated to the student in a timely and transparent manner, with **secretariat@digital4security.eu** copied on the correspondence.

Students may appeal any disciplinary decision in writing within 14 calendar days of formal notification. The appeal must clearly state the grounds for appeal and be submitted via email to **secretariat@digital4security.eu** as well as to the body that issued the original decision.

A formal response shall be issued to the student as early as possible, and no later than four weeks during any active term (excluding the term breaks).

8.4 European and National Codes of Conduct

Beyond the provisions set out in these *Study and Examination Regulations*, the Master's Programme also endeavours to align with the Codes of Conduct and Guidelines of relevant European and national bodies. This includes organisational-level Codes of Conduct, such as Horizon Europe's gender equality provisions and codes for good research practice as defined by the relevant European authorities, while also taking account of national guidance, for example from Germany's DFG.

8.5 Mutual Trust and Shared Responsibility

This programme is built on a foundation of trust. We trust that students are here to grow, learn, and challenge themselves – and that educators are here to support, guide, and inspire.

As a programme, we commit to:

- Clear criteria for every assessment.
- Timely, constructive feedback.
- Respect for cultural, linguistic, and professional diversity.

Students are invited to:

- Engage with honesty and curiosity.
- Ask questions when expectations are unclear.
- Grow not only in expertise, but also in integrity and professional confidence.

Together, we seek to cultivate a learning environment that prepares cybersecurity leaders not only to meet today's challenges, but to shape tomorrow's digital society with responsibility, a mindset of mutual support, collaboration, and confidence.

9. Award of the Joint Master's Degree

9.1 Academic Progression and Award Criteria

To be eligible for the award of the Joint Master's Degree, a student must:

- Successfully complete all 30 ECTS of compulsory components, including the three mandatory taught modules and the Master's thesis;
- Accumulate a total of 60 ECTS (passing a sufficient number of modules by achieving at least 60% of the available total points);
- Comply with any additional requirements outlined in the programme regulations including the Student Agreement, such as adherence to academic integrity standards.

9.2 Pathways by the End of the Designated Study Period

Students who have successfully met all academic and administrative requirements of the programme will be awarded a Joint Master's Degree in Cybersecurity Management and Data Sovereignty, in accordance with the terms set out in the programme's *Cooperation Agreement* (Annex 1).

Students who have not fulfilled all programme requirements within the designated study period must re-register and may be subject to extension fees in accordance with the applicable tuition and fee regulations.

Re-registration is permitted only for students who can complete the programme under current regulations – that is, those who have not failed any mandatory components the maximum number of allowed times (cf. Section 6.4.3). Students who are ineligible for re-registration will exit the programme with a transcript of records detailing all successfully completed components and their corresponding grades. This transcript serves as official documentation of their achievements and lifelong learning. The programme furthermore provides a support service for these

students: If future revisions to the programme structure remove previously mandatory components they failed, the students may be notified about the opportunity to resume and complete their studies.

9.2 Issuance of Academic Documentation

Upon successful completion of the 60 ECTS Online Master's Programme, graduates shall receive the following academic documentation:

- **Joint Degree Certificate** – awarded collectively by the three higher education institutions that are parties to the *Cooperation Agreement* (Annex 1): the German University of Digital Science (UDS, Germany), Munster Technological University (MTU, Ireland), and Universidad Internacional de La Rioja (UNIR, Spain). This certificate confers the degree *Master of Science (MSc) in Cybersecurity Management and Data Sovereignty*.

- **Diploma Supplement** – issued in accordance with the standard format developed by the European Commission, the Council of Europe, and UNESCO/CEPES. Where necessary, the Diploma Supplement shall be amended to meet the relevant national legislative requirements of the awarding institutions.

Document Governance

Amendments to these regulations are subject to consideration and approval by the Master's Board of Directors. Suggestions for refinement can be made by the Admissions and Examinations Board, the Quality Service Committee, student representatives, and other individuals or bodies as appropriate.

Any proposed changes shall be collected and compiled by the Secretariat and prepared for inclusion in the official meeting invitations of the Master's Board, which are distributed at least two weeks prior to the meeting. Proposed changes shall be indicated using track changes in the document. Information on the proposer and the rationale for the change may optionally be included using the comment function.

Correspondence regarding proposed changes shall be addressed to **secretariat@digital4security.eu**, with **masters.board@digital4security.eu** copied in Cc. The Secretariat also supports the Master's Board in monitoring the full set of programme documents to ensure that any substantive changes, i.e. those not of an editorial nature, are duly reflected across all affected documents.

Those who wish to propose changes shall do so with consideration, aiming to submit proposals sparingly and only for well-founded reasons, as the official programme documents are intended to serve as reliable sources of reference. Proposals aimed at eliminating potential inconsistencies, correcting identified errors, clarifying ambiguous formulations, or providing operational details in response to recurring questions are welcome. Such contributions should seek to achieve marginal refinements that preserve the overall structure and integrity of the documents while supporting improvement.

Amendments shall not apply retroactively to academic cohorts already enrolled in the programme, unless it can be reasonably assumed that the amendment is in the students' interest or will not result in any detriment to their academic standing. In particular, no amendment shall adversely affect:

- The overall structure or content of the degree programme as experienced by current students;
- Any academic decision already made about a student's status or progress in the programme.

The Secretariat shall ensure that up-to-date information is available through the programme's designated publication channels.

The current document is designated as *Study and Examination Regulations, Version 1 (V1)*. Editorial changes, such as the correction of spelling errors or the updating of figures that do not alter the manual's meaning, do not affect the version number. Version numbering remains unchanged until student agreements have been signed. Upon official publication, each version shall be dated.

Document Context and Publication

These **Study and Examination Regulations** form part of a comprehensive set of materials that introduce, govern, and support the **60 ECTS Online Master's in Cybersecurity Management and Data Sovereignty**, a fully online joint programme coordinated and delivered by the following three higher education institutions:

- German University of Digital Science (UDS) – Coordinator
  Marlene-Dietrich-Allee 14, 14482 Potsdam, Germany
- Munster Technological University (MTU)
  Rossa Avenue, Bishopstown, Cork T12 P928, Ireland
- Universidad Internacional de La Rioja (UNIR)
  Avenida de la Paz 137, 26006 Logroño, Spain

The programme's structure, academic standards, quality assurance mechanisms, and operational procedures are described across the following documentation package:

Self-Assessment Report - a reference document for external evaluation and accreditation under the European Approach for Quality Assurance of Joint Programmes

I. Governance and Quality Assurance

- Annex 1. Cooperation Agreement
- **Annex 2. Study and Examination Regulations**
- Annex 3. Rules of Procedure for the Master's Board
- Annex 4. Internal Quality Handbook
- Annex 5. Programme Survey Scales
- Annex 6. Industry Advisory Board Manual

II. Curriculum, Learning and Teaching Staff

- Annex 7. Module Handbook
- Annex 8. Student Handbook

- Annex 9. Teaching Staff CVs
- Annex 10. Practical Guide for Lecturers

III. Certification and Recognition

- Annex 11. Sample Degree Certificate
- Annex 12. Sample Diploma Supplement

IV. Administrative and Operational Documents

- Annex 13. Sample Student Agreement
- Annex 14. Sample Supporting Partner Contract
- Annex 15. Sample Remuneration Manual

The programme documentation is maintained as follows:

- **SharePoint** serves as the repository for all programme documents.
- The **Welcome Module** publishes most programme documents (except those requiring protection against forgery or containing confidential information), ensuring transparency for enrolled students and staff.
- The **Digital4Security website** provides open access to selected information for prospective students and other interested parties, including admission requirements and procedures, the course catalogue, examination and assessment regulations, and other key programme details.

No.	Document	SharePoint	Welcome Module	Website
0	Self-Assessment Report	✓	✓	
1	Cooperation Agreement	✓	✓	
2	Study and Examination Regulations	✓	✓	✓
3	Rules of Procedure for the Master's Board	✓	✓	
4	Internal Quality Handbook	✓	✓	✓
5	Programme Survey Scales	✓	✓	
6	Industry Advisory Board Manual	✓	✓	(✓)

No.	Document	SharePoint	Welcome Module	Website
7	Module Handbook	✓	✓	(✓)
8	Student Handbook	✓	✓	✓
9	Teaching Staff CVs	✓	✓	
10	Practical Guide for Lecturers	✓	✓	
11	Sample Degree Certificate	✓		
12	Sample Diploma Supplement	✓		
13	Sample Student Agreement	✓	✓	
14	Sample Supporting Partner Contract	✓		
15	Sample Remuneration Manual	✓		

In the event of inconsistencies or conflicting interpretations among these documents, the following **order of precedence** applies:

1. Cooperation Agreement
2. Study and Examination Regulations
3. Rules of Procedure for the Master's Board
4. Internal Quality Handbook
5. Module Handbook
6. Student Handbook
7. Student Agreement
7. Programme Survey Scales
8. Supporting Partner Contracts
9. Other supporting documents

This hierarchy, as officially defined in the *Cooperation Agreement*, serves to ensure that foundational arrangements and formally adopted regulations take precedence over illustrative or operational materials.

Should the reader become aware of, or suspect, any inconsistency or misalignment between the documents, please contact **Secretariat@digital4security.eu**.

Together, these materials form the backbone of a transformative joint programme that seeks to integrate academic excellence, industry relevance, and social responsibility. It reflects the shared commitment of academic leaders, instructors, students, industry experts, and partner institutions, to shaping a student-centred, accessible, and future-oriented study environment.

This collective effort supports:

- **Empowering cybersecurity leaders** with the capacity to anticipate and manage risks, while collaborating effectively across stakeholders;
- **Delivering high-quality, flexible online learning** grounded in real-world application;
- **Supporting lifelong learning and workforce adaptability** in a rapidly evolving digital landscape;
- **Aligning education with industry and market needs** to ensure professional relevance;
- **Facilitating European strategic autonomy** through digital sovereignty and resilient infrastructure;
- **Advancing inclusion, accessibility, and gender equality** in the cybersecurity field; and
- **Promoting responsible innovation, ethics, and regulatory compliance** in all aspects of digital security.

We thank all contributors for their continued collaboration in advancing the **Digital4Security** vision: to empower learners, institutions, and societies in shaping a more secure, inclusive, and sovereign digital future.

Project 101123430 — Digital4Security — DIGITAL-2022-SKILLS-03

Digital4Security

Shaping Europe's cyber future

ADVANCED DIGITAL SKILLS

DIGITAL EUROPE PROGRAMME

Co-funded by the European Union