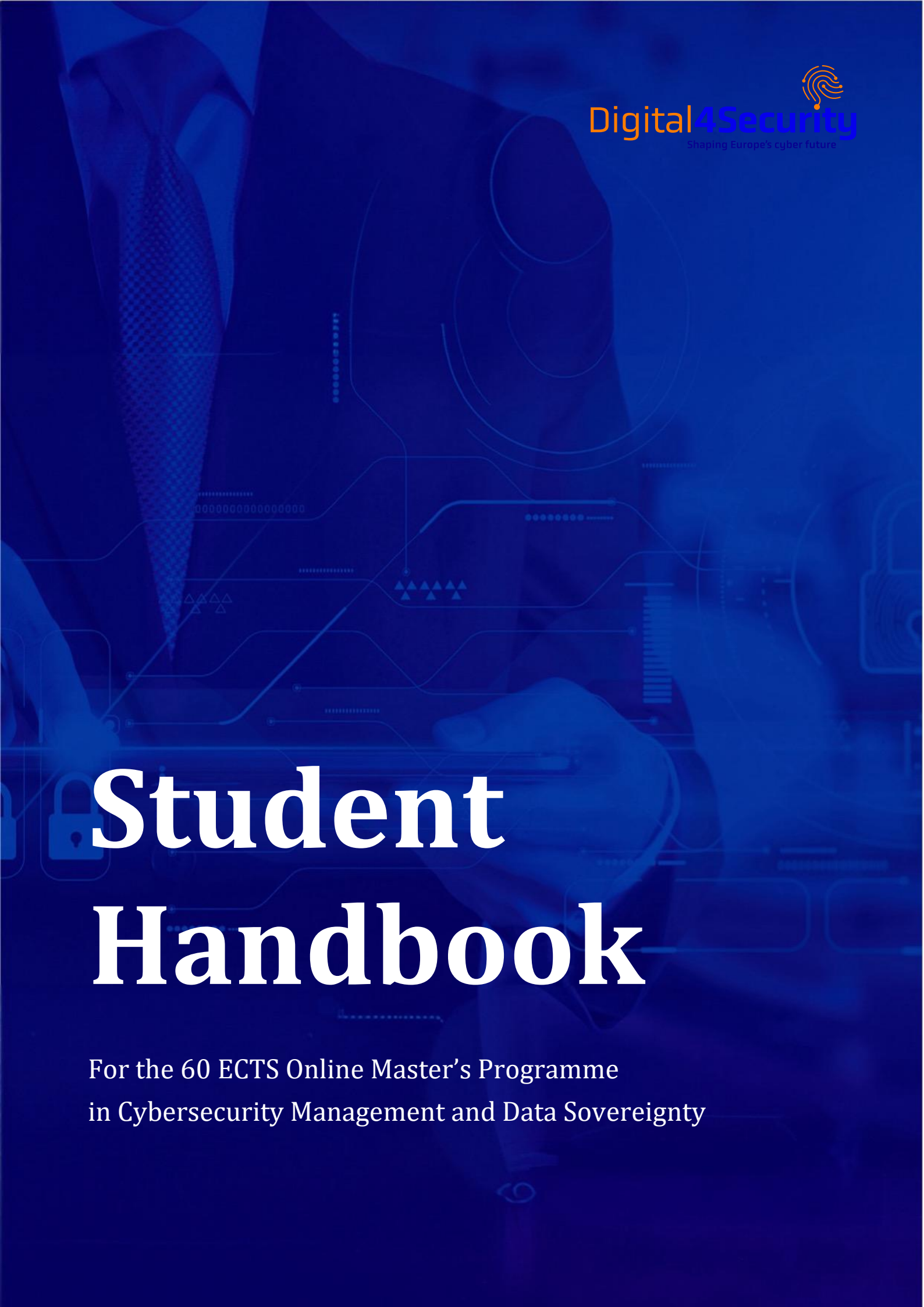


Digital4Security
Shaping Europe's cyber future

Student Handbook

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

Table of Contents

1. Welcome to the Joint Master's Degree Programme in Cybersecurity Management and Data Sovereignty (60 ECTS, Online)

We are delighted to welcome you to the **Joint Master's Degree Programme in Cybersecurity Management and Data Sovereignty**, a European postgraduate degree offering innovative and flexible learning pathways for the next generation of cybersecurity leaders.

The curriculum combines essential technical capabilities with a strong emphasis on strategic management, regulatory compliance, and organisational resilience. The programme equips you with the interdisciplinary skills required to lead secure digital transformation across sectors. You will engage with a wide range of topics across three content pillars:

- **Management, Governance and Compliance**
- **Organisational and Industry Resilience**
- **Cybersecurity Operations and Technologies**

Designed with a European labour market focus, the programme provides you with the **advanced digital and managerial skills** that are highly sought after in today's fast-evolving digital economy, particularly among **Small and Medium-sized Enterprises (SMEs)** and **public sector organisations**. These skills are essential for enabling secure digital transformation, navigating complex regulatory environments, and strengthening cyber resilience across sectors.

The programme is offered as a **60 ECTS, fully online degree**, jointly awarded by:

- German University of Digital Science (Coordinating Institution, UDS, Germany).
- Munster Technological University (MTU, Ireland).
- Universidad Internacional de La Rioja (UNIR, Spain).

This collaborative programme was developed under the **EU co-funded Digital4Security project**, directly addressing the growing need for **cybersecurity professionals who can lead, manage, and implement secure digital strategies** across Europe's private, public, and non-profit sectors.

We are excited to have you on board and look forward to supporting you throughout your studies. We hope you find the programme engaging and deeply rewarding.

Welcome to your Digital4Security journey!

1.1 About This Handbook

This handbook is designed as a companion to support you throughout your academic journey. It provides guidance and key contacts to help you navigate your studies. Here, you will find essential information, allowing you to:

- Discover the partners in the Digital4Security project and how each of them may offer valuable opportunities for you.
- Explore the curriculum, different study tracks, and the academic calendar.
- Learn how to apply, enrol, and get started smoothly.
- Navigate assessments, exams, and academic integrity with confidence.
- Understand how the programme is governed and what legal frameworks apply.
- Get involved through student representation and community-building initiatives.
- Access a wide range of student services designed to support your growth and success.
- See how quality is assured, and your feedback makes a difference.
- Become familiar with the digital learning environment.
- Find practical tips for managing your studies.
- Prepare for graduation and celebrate it.
- Know whom to contact when you need help or advice.

While this handbook offers an overview, you may also wish to explore the following additional resources. An overview of where to find what is included at the back of this document.

- The **Module Handbook** provides a detailed introduction to each module, including the content, workload, and assessments.
- The **Study and Examination Regulations** contain key information on the application process, assessment and grading procedures, course progression, academic conduct, as well as complaints and appeals.

- The **Internal Quality Handbook** explains how the programme maintains high academic standards. It outlines the programme's overarching goals, feedback processes, as well as the mechanisms in place to support student satisfaction and success.
- The **Teaching Staff CVs** offer an overview of the individuals involved in delivering the programme, their academic backgrounds, research interests, and the courses they teach.
- The **Welcome Module** on the Learning Platform helps you to get started smoothly with the programme. It includes videos on platform navigation, tips for online study, guidance on how to reference AI-generated content, and more. Section 15 below offers further detail.

We invite you to make use of those resources as needed, reaching out to our support team via **studyaffairs@digital4security.eu** if you have any questions or suggestions.

You are not only joining a degree programme, but becoming part of a vibrant, international community of learning, research, and professional practice. We are committed to supporting your growth, leadership, and success. We also warmly invite you to actively contribute in shaping a culture of collaboration, curiosity, and mutual support, united by the shared goal of advancing cybersecurity and digital resilience.

1.2 Meet the Programme Leaders

I am excited to welcome you to the Digital4Security Online Master's programme. As the head of the EU-funded Digital4Security project, my vision is to empower you with both cutting-edge academic knowledge and practical industry certification. Through this programme, you will develop the leadership and technical skills needed to protect Europe's organisations, especially SMEs, from ever-evolving cyber threats. Together, we will build a more resilient, secure digital future. Welcome aboard!

Prof. Dr. Ciprian Dobre, Vice Rector, Head of the Digital4Security EU project, University Politehnica of Bucharest (UPB)

Prof. Dr. Julia von Thienen, Programme Director, German University of Digital Science (Master's Programme Coordinating Institution, UDS)

Welcome! This fully online Master's is designed not only to build your expertise, but also to create a collaborative culture where you can form lasting connections with peers and institutions for years to come. Many of you may be preparing for leadership roles, and the programme itself aims to model inclusive leadership: valuing diverse skills, encouraging curiosity, and fostering teamwork that sparks both personal growth and joint opportunities. You are not here as a passive learner. You are invited to take initiative, share ideas, and even help shape the programme itself. Together, we can drive innovation in real-world cybersecurity practice.

Welcome – I'm delighted you've joined us. This programme sits at the intersection of business resilience and cybersecurity, where awareness meets real-world decision-making. While many cybersecurity programmes deliver technical proficiency, this master's also cultivates your legal, regulatory, and compliance skills, enabling you to navigate confidently from rules and risk to effective board-level actions. You'll learn not just what needs to be done, but how to implement it in organisations, designing for real impact and safety. Make the most of projects, partnerships, and peer networks – bring your questions, ideas, and challenges into the classroom. We look forward to seeing what you build and how you help shape safer, more resilient organisations.

Jacqueline Kehoe, Programme Director, Munster Technological University (MTU)

Prof. Dr. Fidel Paniagua Diez, Programme Director, Universidad Internacional de La Rioja (UNIR)

Welcome, I'm excited to have you with us! This programme offers a fascinating blend of perspectives on cybersecurity. While the curriculum emphasizes management outlooks, a strong grasp of technical concepts is likewise important for making informed decisions, and leading with confidence in today's complex cybersecurity landscape. A unique benefit of this programme is its flexibility: you can shape your own pathway, choosing whether to cover the technical dimensions broadly, or take dedicated modules to explore topics in greater depth. In addition, the programme provides ample applied opportunities where you can bring your skills to bear in real-world contexts, making a difference when it matters.

1.3 Who This Programme Is Designed For

The Joint Master's Degree in Cybersecurity Management and Data Sovereignty is designed for ambitious professionals who want to deepen their expertise and take the next step in their cybersecurity careers, without putting their lives on hold.

Whether you are already working in IT, law, compliance, risk management, or business leadership, or seeking to transition into cybersecurity from a related field, this programme offers a flexible, high-impact learning path tailored to your professional goals.

1.3.1 Who Typically Joins This Programme?

Based on industry needs and student feedback, our programme is ideally suited for:

- **Business leaders and entrepreneurs** who want to safeguard their organisations against cyber threats and ensure GDPR compliance,
- **IT professionals and engineers** aiming to move into strategic leadership roles like Chief Information Security Officer (CISO) or cybersecurity manager,
- **Compliance or risk management experts** looking to gain technical foundations in cybersecurity, bridging the gap between policy and protection,
- **Career changers** from adjacent fields seeking to upskill in a fast-growing sector,

- **Mid-career professionals** balancing work, family, and education – looking for flexibility, relevance, and real career benefits.

What is Cybersecurity?	What is Data Sovereignty?
Cybersecurity refers to the protection of digital systems, networks, and data from unauthorised access, disruption, or damage. In this programme, you will explore cybersecurity not only as a technical challenge, but also as a strategic responsibility – essential for ensuring business continuity, regulatory compliance, and trust in digital operations.	Data sovereignty concerns the control over data according to the laws and governance frameworks of the country or region where the data is stored or processed. This programme approaches data sovereignty as a key leadership issue, connecting legal, ethical, and technical perspectives to help organisations navigate global compliance and safeguard digital autonomy.

Whatever your path, if you are seeking **advanced digital skills with a management focus in the fields of cybersecurity or data sovereignty**, this programme is for you.

1.3.2 Programme Design That Fits Your Life

The structure of this Master's programme has been carefully designed to support real-life learners: professionals who may balance work, family, and education, or who are transitioning into new roles and responsibilities. Key programme features include:

- Fully online delivery, accessible from anywhere.
- Modular, "bite-sized" learning that supports flexible pacing.
- Both part-time and full-time study options to fit your lifestyle.
- Career pathways linked to professional roles (e.g. Chief Information Security Officer, Cyber Risk Manager, Cybersecurity Auditor).

- Industry-aligned curriculum, developed in close cooperation with employers and grounded in real-world cybersecurity scenarios.

You may select modules aligned with your intended career path or combine them to create your own unique learning journey. Your professional focus and pathway will be documented in your **Diploma Supplement**, while the final award will be a **Master of Science**, jointly conferred by UDS (Germany), MTU (Ireland), and UNIR (Spain). The programme is currently undergoing EU-accreditation by the prestigious agency ASIIN (see Section 11.4).

We understand that plans can change. If your priorities shift during your studies, you may exit the programme after earning 30 or more ECTS and receive a **Postgraduate Certificate**. Should you later decide to continue, you can re-enrol and pick up where you left off. Modules you have already completed are normally recognised straight away, so you can carry on seamlessly towards finishing your degree. More information is available in Section 5.5.

1.3.3 Industry Certification

In addition to your academic Master of Science degree, you will have the opportunity to earn **industry-recognised certifications**, demonstrating your readiness for specific professional roles in SMEs or public sector organisations.

Modules include recommendations for relevant certification options. If you choose to pursue certification, you will gain access to targeted self-study materials, mock exams, and exam preparation tools. These certifications are **aligned with the European Cybersecurity Skills Framework (ECSF)** and will enhance your visibility and employability in today's competitive digital job market.

You may complete industry certifications aligned with modules completed, while in some cases, recommended certifications can be undertaken before the start of the Master's to provide a solid grounding in key subject areas. As a student of the programme, you will also benefit from special rates on selected certifications.

1.3.4 Alternative Study Options

If you are considering a future academic career, such as pursuing a PhD, or if you are seeking more extensive training beyond a 60 ECTS programme, you may be interested in the **sister programme** of this online Master's degree: a **120 ECTS hybrid Master's in Cybersecurity Management and Data Sovereignty**, coordinated by the **National University of Science and Technology POLITEHNICA Bucharest**[1], also developed within the framework of the **Digital4Security** project.

Both programmes are closely interconnected. If you complete the 60 ECTS online Master's degree, you may later choose to enrol in the 120 ECTS programme, with all your previous academic achievements fully recognised. This pathway may be particularly relevant if you wish to earn additional ECTS credits required for entry into certain PhD programmes or other advanced academic pursuits.

[1] https://upb.ro/

2. Digital4Security

The **60 ECTS Online Master's in Cybersecurity Management and Data Sovereignty** is part of a broader educational initiative developed through the **EU co-funded Digital4Security (D4S) project**. This initiative brings together leading European universities, research centres, and industry partners to address the growing demand for highly skilled cybersecurity professionals across Europe, especially in **Small and Medium-sized Enterprises (SMEs)** and public institutions.

The 60 ECTS Online Master's Programme was created in close collaboration with over 30 partners across Europe, as listed in Table 1.

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

No.	Partner	Abbreviation	Country	Role
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
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

No.	Partner	Abbreviation	Country	Role
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

2.1 A European Response to Cybersecurity Needs

The Digital4Security project is part of the **DIGITAL Europe Programme** and is designed to develop **innovative, effective, and sustainable education at master's level**. It combines **managerial, regulatory and technical content** to prepare students for leadership roles in cybersecurity. The curriculum is tailored to meet real-world needs and was developed with direct input from employers, ensuring its relevance in today's rapidly evolving digital landscape.

Graduates of Digital4Security study programmes will be equipped to:

- Lead cybersecurity initiatives within organisations.
- Assess and respond to emerging cyber threats.
- Ensure compliance with European data protection and cybersecurity laws.
- Implement strategic and resilient digital infrastructures.

2.2 Flexible Study Options for Diverse Learners

The **60 ECTS Online Master's Programme** was specifically designed for **mid-career professionals**, **career changers**, and **working learners** who require a flexible, modular, and practice-oriented academic experience. This programme allows you to

balance professional, personal, and academic responsibilities while advancing your career in cybersecurity management and data sovereignty.

For those seeking more extensive academic training, or planning to pursue a PhD, the **120 ECTS Hybrid Master's Programme**, coordinated by the **National University of Science and Technology POLITEHNICA Bucharest**, offers a longer study format with a combination of online and on-campus components.

A comparison between the two Digital4Security Master's programmes is offered in Table 2.

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)

Aspect	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)

While the 60 ECTS Online and 120 ECTS Hybrid Master's programmes differ in format and scope, they are both part of the same coordinated initiative and offer several shared benefits, including:

- Access to the **Digital4Security learning platform** for enrolment, course participation, and educational resources.
- Participation in **joint events**, including guest lectures, weekend seminars, and networking opportunities.
- Collaboration with a **European Industry Advisory Board**, ensuring ongoing alignment with labour market needs and professional expectations. You can find a list of the partners involved in the **Industry Advisory Board Manual**, with access guidance provided by the end of this document.

These shared elements foster a strong sense of community across programmes and ensure that all learners benefit from a common European foundation of cybersecurity excellence.

2.3 Beyond the Degree: Skills That Matter

Participants in the Digital4Security study programmes benefit from a strong connection between academic learning and professional application. The Digital4Security study programmes offer:

- Mentoring by faculty and industry experts.
- Hands-on, project-based learning.
- Preparation for industry certifications.
- Access to real-world tools, platforms, and scenarios used in cybersecurity practice.

This educational approach helps to ensure that students graduate with more than an academic degree. You gain **practical skills, recognised credentials, and access to a network of European cybersecurity professionals**.

2.4 The Degree-Awarding Universities: Three Homes Across Europe

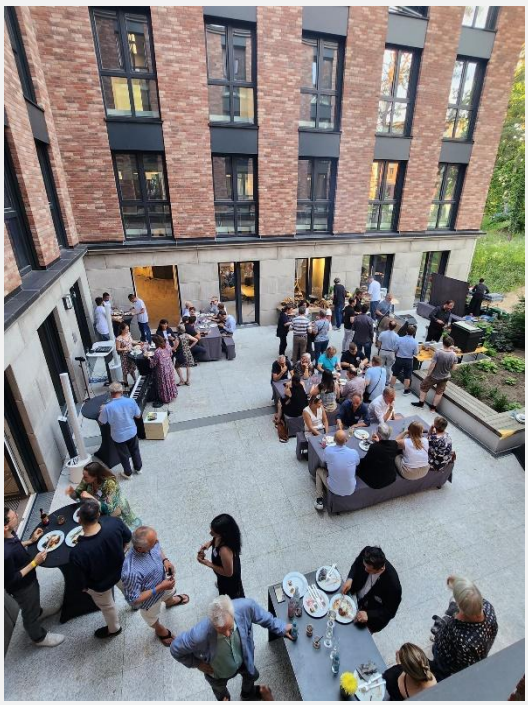
The **60 ECTS Online Master's Programme in Cybersecurity Management and Data Sovereignty** is jointly awarded by three universities:

- **German University of Digital Science (UDS, Germany).**
- **Munster Technological University (MTU, Ireland).**
- **Universidad Internacional de La Rioja (UNIR, Spain).**

Throughout your studies, you will primarily use the **Digital4Security** learning platform (described in Section 14), which provides a unified virtual space for your entire learning experience. Behind this digital environment stand three real-world institutions: UDS, MTU, and UNIR. They serve as your **academic homes**, contributing to teaching, supervision, and academic support. In this way, you will have three base stations across Europe, **in Germany, Ireland, and Spain**.

In addition to these three core institutions, the wider **Digital4Security network** includes many other partner organisations. As part of your learning experience, you may engage with them through individual modules, weekend workshops, or networking events. All of them can be attended virtually, but you may also choose to participate in one or the other on-site.

The opportunities for visiting your three home universities vary. While UDS and UNIR are both fully online institutions, delivering all regular classes remotely, UDS also offers Career Weeks (Section 17.3): optional short-term stays in Potsdam, Germany, where students can attend workshops at the university headquarters and complete brief internships with local companies. MTU even operates a large physical campus. If you enjoy walking the physical campus of a home university, MTU may be a great place to visit. UNIR, meanwhile, offers special on-site events such as graduation ceremonies, giving students the chance to celebrate the completion of their online studies in a festive and shared live experience (see Section 16.2).



The **German University of Digital Science** (UDS) headquartered in Potsdam, Germany, is a forward-looking higher education institution committed to driving responsible digital transformation. As a fully online university, UDS makes state-of-the-art German higher education globally accessible through flexible, remote delivery. All academic programmes are taught in English and focus on high-demand digital fields, such as cybersecurity, artificial intelligence, and emerging digital technologies. UDS's innovative educational model integrates academic excellence with practical, hands-on learning. It fosters a dynamic online learning community through immersive virtual labs, design thinking projects, and an interactive 3D virtual campus. This approach ensures a rich and engaging educational experience, purpose-built for the needs of a digitally connected and rapidly evolving world.

Munster Technological University (MTU), located in Ireland, is a self-awarding university known for its strong emphasis on applied research and industry collaboration. MTU offers a range of programs in cybersecurity, including a full-time MSc in Cybersecurity and a part-time, fully online MSc in Cybersecurity Management. These programs are designed to equip students with both technical and managerial skills, preparing them for leadership roles in the cybersecurity sector. MTU promotes flexible learning and real-world integration across its curriculum. With campuses across the south of Ireland and a dynamic research ecosystem, MTU plays a leading role in innovation and skills development in the region and beyond, particularly in areas such as cybersecurity, digital transformation, and enterprise resilience.

The **Universidad Internacional de La Rioja** (UNIR), headquartered in Logroño, Spain, is a leading online university specializing in distance education. With a student body exceeding 90,000 across more than 80 countries, UNIR offers a wide array of programs, including specialized courses in cybersecurity. The university's Research Institute for Innovation & Technology in Education (UNIR iTED) holds a UNESCO Chair on eLearning and is actively involved in numerous R&D projects focused on educational technology. UNIR offers extensive expertise in online teaching and is committed to integrating practical, real-world experiences into its programs. The university offers Bachelor's, Master's, and Doctoral programmes across a wide range of disciplines, and maintains a strong IT department, including education in cybersecurity and related fields.

Figure 1 provides you with a brief overview of where your academic homes are located across Europe.

While the study programme is delivered entirely online, you will be affiliated with UDS (headquartered in the Berlin-Potsdam area, Germany), MTU (headquartered in Cork, Ireland), and UNIR (headquartered in Logroño, Spain). You are never required to attend any event or procedure on site, but these locations may well be worth a visit.

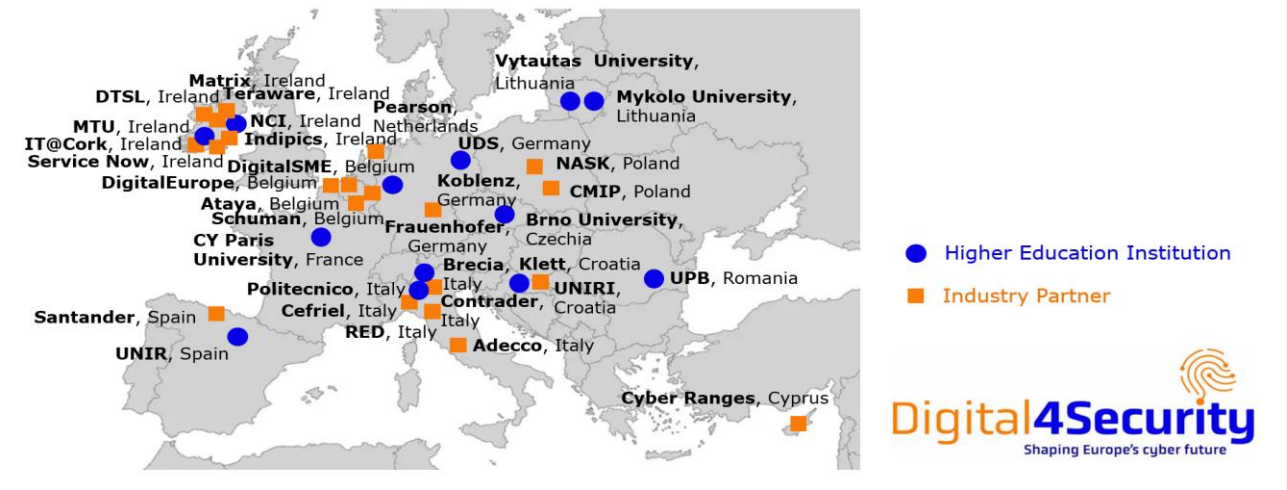
Figure 1: Your Academic Home Universities Across Europe.

2.5 Partners Across the Digital4Security Network:

Mentors and More

The **Digital4Security network** spans institutions and organisations across Europe, bringing together a diverse community of universities, research centres, SMEs, and leading industry players (see Figure 2). This strong international foundation is one of the programme's greatest assets – giving you access to a wide array of expertise, experiences, and opportunities beyond your home universities.

Figure 2: The Digital4Security Network Connects You to Higher Education Institutions and Industry Partners Across Europe.



Partner organisations contribute in many ways to enrich your learning experience and support your professional development. Their involvement goes far beyond academic instruction. In addition to helping deliver modules, partners may offer guest lectures, hands-on workshops, cyber challenges and simulations, hackathons, webinars, and networking events. Some also organise bootcamps, internships, and job placement opportunities, helping you build both skills and connections within the European cybersecurity landscape.

Many partners are actively involved in **student mentoring and feedback**, offering guidance that draws from both academic insight and practical experience. Others contribute behind the scenes – supporting the master's programme through outreach, communications, platform development, layout and design, technical support, or financial coordination.

Finally, partner institutions play a key role in **quality assurance**, helping to ensure that the programme remains relevant and responsive to the evolving cybersecurity needs of European industries and public sector organisations.

In short, the Digital4Security partner network is here not only to support your studies, but to serve as a **rich, real-world ecosystem of mentors, collaborators,**

and professional contacts, ready to accompany you on your journey into cybersecurity leadership.

Below you find a brief overview of the institutions involved. Get ready to explore this incredible **network of partner institutions**: some of the most exciting destinations for virtual exchange, online collaboration, and real-world impact in cybersecurity and digital leadership.

2.5.1 Academic Partners (Higher Education Institutions)

Brno University of Technology (Czech Republic)
Explore one of Central Europe's top technical universities, offering hands-on cybersecurity labs, digital forensics training, and real-world CTF competitions. A great choice for students who want to learn by doing, even remotely.

CY Cergy Paris Université (France)
At the outskirts of Paris, CY offers a strong interdisciplinary profile and international flair. Expect inspiring online courses, rich research networks, and an ideal launchpad for European virtual mobility.

German University of Digital Science (Germany)
A fully digital, next-gen university focused on AI, digital transformation, and applied tech. If you are a remote learner interested in driving innovation and exploring new perspectives in cybersecurity, data science, and digital leadership, UDS is built for you.

Munster Technological University (Ireland)
Based in vibrant Cork, MTU offers a great mix of real-world projects and remote learning. Their digital innovation labs and strong industry links make them a fantastic base for tech and business-savvy students.

Mykolo Romerio University (Lithuania)
MRU leads in law, public governance, and now digital security. With flexible

online modules and a strong European network, it is a brilliant pick for those interested in legal and economical sides of cybersecurity.

National College of Ireland (Ireland)
NCI combines tech, business, and leadership in the heart of Dublin's tech district. Their modern e-learning approach and career-focused courses make it a great fit for future cybersecurity leaders.

Politecnico di Milano (Italy)
One of Europe's most prestigious tech universities. Their "Cyber Risk Strategy & Governance" program (co-run with Bocconi) is world-class. Expect high-level content, global networking, and strong online options.

Universidad Internacional de La Rioja – UNIR (Spain)
Spain's leading online university, with top-tier digital platforms, flexible schedules, and strong academic support. Perfect for students looking to specialize in cybersecurity fully online.

Università degli Studi di Brescia (Italy)
UNIBS blends technical excellence with strong social values and legal expertise. Their research in smart technologies, online education, and law make them an attractive stop on your virtual mobility journey.

National University of Science and Technology POLITEHNICA Bucharest (Romania)
The project coordinator and a powerhouse in technical education. UPB offers cutting-edge expertise in cybersecurity, smart cities, and online engineering education. A great anchor for ambitious students.

Universität Koblenz (Germany)
A specialist in informatics, data science, and digital transformation. UNI KO is an excellent choice for students looking to dive into applied digital research through hybrid and online study formats.

University of Rijeka (Croatia)
A coastal gem combining Mediterranean charm with digital innovation. Rijeka is all about multidisciplinary learning and active student participation, online or on-site.

Vytautas Magnus University (Lithuania)
A progressive university rooted in liberal arts values and open science. VMU promotes international cooperation and modern online teaching formats, ideal for cross-cultural digital learners.

2.5.2 Associate Partners

Adecco (Italy)
A global employment leader focused on future skills. Connect to virtual or on-site cybersecurity bootcamps and remote talent programs.

Ataya & Partners (Belgium)
Experts in digital strategy, public-private partnerships, and cross-border collaboration. Great if you are curious about cybersecurity policy and innovation ecosystems.

Banco Santander (Spain)
More than just a bank - Santander supports education through scholarships, virtual internships, and global student opportunities in fintech and security.

Cefriel (Italy)
A Milan-based hub linking research and industry. Join digital co-innovation labs and virtual hackathons with real-world impact.

CMIP – CyberMadeInPoland (Poland)
This national cluster connects companies and universities in cybersecurity. Perfect for virtual networking with Europe's cyber innovation scene.

Contrader (Italy)
An IT services company working on next-gen tech, including AI, digital identity, and smart mobility - great for student collaborations and online R&D.

Cyber Ranges Ltd (Cyprus)
Creators of next-level cyber training environments. Their cloud-based platforms let you simulate attacks, defense, and incident response: all online.

DIGITALEUROPE (Belgium)
The voice of Europe's tech industry. They promote digital skills, gender equality, and policy innovation. Watch for exciting online events and student challenges.

Digital Technology Skills Ltd (Ireland)
Helping people thrive in the digital workplace with micro-credentials, certifications, and tailored cybersecurity training.

Digital SME Alliance (Belgium)
The largest network of digital SMEs in Europe. They advocate for small tech companies and provide opportunities for students to engage with the real digital economy.

Fraunhofer-Gesellschaft (Germany)
Europe's top applied research organization. With a focus on security, AI, and future tech, they offer world-class digital learning and virtual labs.

Independent Pictures (Ireland)
Digital media experts who bring storytelling into learning. Great for students interested in educational videos, campaigns, or documentary-style content.

IT@Cork (Ireland)
An energetic tech community hosting online workshops, innovation days, and meetups - ideal for virtual networking with Irish industry leaders.

Matrix Internet (Ireland)
A creative digital agency offering insights into web development, UX, and digital transformation - experienced collaborators in EU-funded learning projects.

NASK (Poland)
A national research institute that powers Poland's internet and cybersecurity infrastructure. Great for students interested in national cyber defense and policy.

Pearson Benelux (Netherlands)
A major player in digital education, offering online learning content and assessment tools used worldwide.

Profil Klett (Croatia)
An innovative educational publisher creating digital content and teacher tools - helping to build foundational digital skills from the ground up.

Red Open (Italy)
Experts in open innovation and digital culture. Join their virtual labs and design sprints that bring people, ideas, and solutions together.

Schuman Associates (Belgium)
EU funding and policy specialists. They support online training in strategic communication, funding access, compliance and digital policy.

ServiceNow (Ireland)
The workflow engine behind many of the world's biggest companies. Learn how to automate, secure, and improve digital services, online and on demand.

Skillnet (Ireland)
A national agency committed to fostering innovative workforce development. Empowers students to meet the ever-evolving needs of industry and society.

Terawe Technologies (Ireland)

Specialists in AI, cloud, and immersive tech. Their platforms support hands-on learning in virtual environments - great for future-ready students.

3. Programme Overview

Ready to dive into your studies?

The following sections give you a concise overview of the degree programme.

You can also find a video introducing this content in the **Welcome Module**.

3.1 Title Awarded

This joint master's programme leads to the internationally recognised degree:

Master of Science (MSc) in Cybersecurity Management and Data Sovereignty.

Upon successful completion, your degree will be **jointly awarded** by three European universities:

- **German University of Digital Science (UDS)**, Germany.
- **Munster Technological University (MTU)**, Ireland.
- **Universidad Internacional de La Rioja (UNIR)**, Spain.

These three institutions collaboratively design, deliver, and oversee the programme. Each of them also contributes one core mandatory module, ensuring you benefit from the strengths and specialisations of all three. Furthermore, each awarding university offers two professional pathways designed to support your career goals with tailored guidance and preparation.

3.2 Partner Institutions and Their Roles

This joint programme is part of the broader **Digital4Security** initiative, involving a large network of universities and industry partners across Europe. While UDS, MTU, and UNIR are the awarding institutions, you will encounter lecturers and mentors from other academic partners as well.

The **Digital4Security platform** (Section 14) provides one unified learning environment, giving you access to resources, support, and virtual classrooms shared by all participating institutions.

3.3 Study Options for Full-Time and Part-Time Learners

The programme comprises **60 ECTS credits**, equivalent to approximately 1,500 hours of total student work. One ECTS credit corresponds to a workload of approximately 25 hours, including lecture participation, practical exercises, self-study, and exam preparation.

The programme is designed with flexible delivery options to fit diverse lifestyles and career stages:

- **Full-time**: Complete the degree in **1 year** (3 terms)
- **Part-time accelerated**: Complete in **1¼ years** (4 terms)
- **Part-time**: Complete in **2 years** (6 terms)

You may switch between tracks during the course of your studies, depending on your evolving needs. This may entail fee changes as transparently explained on the website.

Figures 3-5 provide a visual overview of the typical distribution of taught modules and the final thesis across each of the three delivery tracks.

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

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

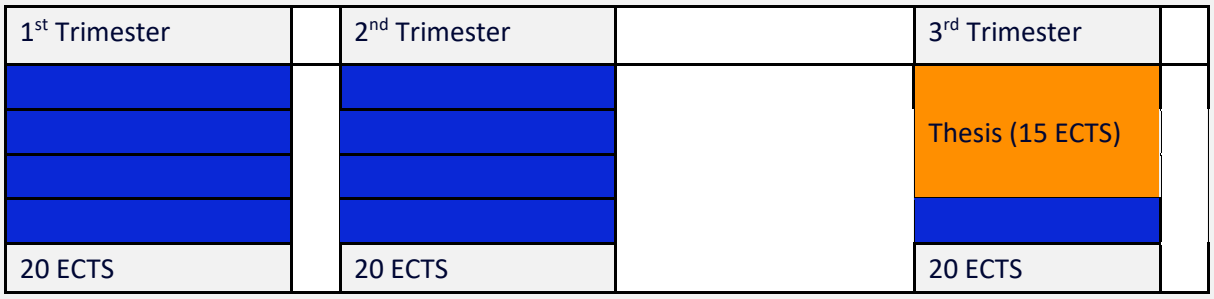


Figure 4: Part-Time Accelerated Track (1¼ Years / 4 Terms / 15 ECTS per Term).

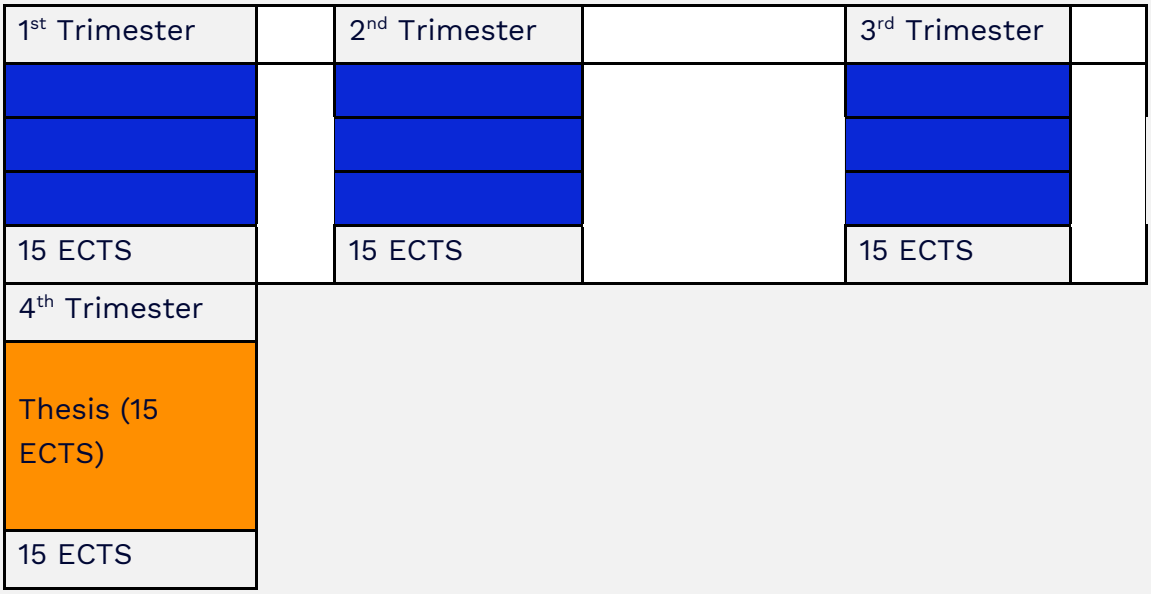


Figure 5: Part-Time Track (2 Years / 6 Terms / 10 ECTS per Term).

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

3.4 Optional Fast-track Full-Time: 30 ECTS Per Term

While the standard study plan is based on completing **20 ECTS per term** for full-time students, corresponding to around 40 hours of weekly workload, the programme offers flexibility for students who wish to **fast-forward their studies**. If you are ready to dedicate more time, you may choose to take **30 ECTS per term**, completing all coursework in just two terms, that is 2 x 12 teaching weeks, plus exam weeks.

Since mandatory modules are concentrated in the first two terms and **thesis supervision is available year-round**, this structure allows you to take on your thesis already in the second term and complete the programme ahead of schedule.

*Please note, however, that this path requires a significant commitment: Students should be prepared for a **weekly study workload of approximately 60 hours**. This option may suit students who are highly motivated, who have only a short window away from professional duties and thus aim to progress quickly through concentrated study, and who demonstrate strong time management skills.*

Please also note that this is not an official study track, but it can be a private decision to fast-forward your studies by concentrating all your efforts in a condensed time-period, in order to be extra-fast.

If you are considering this route, we encourage you to **discuss your plan in advance with the Programme Coordinator** responsible for your chosen professional profile. They can help you assess feasibility and offer guidance on balancing your workload effectively.

3.5 Language of Instruction

The entire programme is taught and assessed **in English**. To participate effectively, a **minimum English proficiency of CEFR B2** is required. For more details on accepted language certificates, please see Section 5 on the admissions process.

3.6 Programme Structure

The programme comprises 60 ECTS, which are structured as follows:

- **15 ECTS** – Mandatory taught modules (one from each awarding university)
- **15 ECTS** – Electives aligned with your chosen professional profile (optional)
- **15 ECTS** – Freely chosen electives (including the option to stack micro-credentials)
- **15 ECTS** – Master's thesis

Each taught module is worth **5 ECTS** and may include various learning formats such as video lectures, live seminars, teamwork, case studies, and project work.

The curriculum with its learning outcomes is described Section 4 below.

3.7 Professional Profiles: Tailoring Your Learning Path

The Digital4Security Master's Programme is designed to address the diverse needs of students while staying closely aligned with the evolving demands of the European cybersecurity landscape. The curriculum draws on role profiles defined by the **European Union Agency for Cybersecurity (ENISA)** to ensure that your studies prepare you for real-world, high-demand roles in the field.

To support this, the programme offers a selection of **specialised professional profiles**, each curated by one of the three awarding universities, based on institutional expertise. Each institution leads two profiles and provides associated guidance – including academic supervision, suggestions for relevant industry certifications or events.

While not every profile may be offered at all times (depending on overall student numbers), **once you select a profile during the admission process**, dedicated support for that profile is guaranteed throughout your studies, **for up to five years**.

The following professional profiles are supported by the curriculum:

- **Chief Information Security Officer (CISO)** – curated by UDS
- **Cyber Legal, Policy, and Compliance Officer** – curated by MTU
- **Cybersecurity Risk Manager** – curated by MTU
- **Cyber Threat Intelligence Specialist** – curated by UNIR
- **Cybersecurity Educator** – curated by UDS
- **Cybersecurity Auditor** – curated by UNIR

You can find more information about each of these profiles in a systematic description of *European Cybersecurity Skills Framekwork (ECSF) Role Profiles* available for **download**.

Within the master's programme, each profile is associated with **5 to 10 recommended modules**. Students who complete at least **15 ECTS** from these recommended modules will receive formal recognition of their profile preparation in their **Diploma Supplement**.

Choosing a professional profile is optional. If you prefer, you can freely select all 30 of your elective ECTS without committing to a specific profile. However, we strongly recommend that you align your module choices with your intended career path by selecting a profile. Doing so gives you access to **tailored preparation, career guidance, and enhanced documentation of your specialisation**, which can be valuable assets for your future employers or academic pursuits.

3.7.1 How to Sign up for a Professional Pathway?

You can choose your **Professional Pathway** during the **admission process**, simply by selecting the profile that best aligns with your career goals.

If you did not select a pathway at admission, you can **sign up** later by contacting the **Programme Coordinator** of the university curating your preferred profile.

If your goals evolve during your studies, you are welcome to change your selected **Professional Pathway**. To do so, please contact **both** Programme Coordinators – of the profile you wish to leave and the one you would like to join – by sending a **single email** addressed to both. This ensures a smooth handover and proper documentation of your updated study focus.

3.7.2 How Will Your Professional Pathway be Documented?

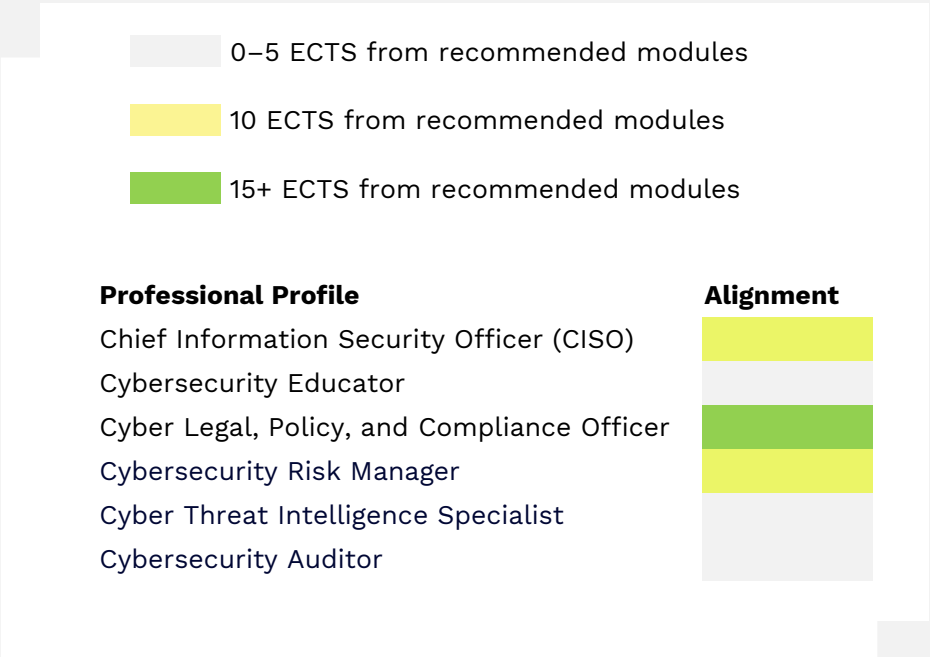
Your Diploma Supplement will officially emphasize **one professional profile** – the one you were enrolled in at the time of completing your studies – provided you have earned at least 15 ECTS from its recommended modules. This highlights your

focus on a specific career goal, for which you also received tailored support during the programme.

In addition, the Diploma Supplement will include a **visual diagram**, showing how your completed modules align with all profiles supported by the programme. Each profile will be marked to indicate the level of match in relation to the recommended modules.

The diagram helps demonstrate how your learning supports different professional roles, alongside a **full list of all completed modules and percentage points earned**, giving future employers and institutions a clear overview of your strengths and competencies. An example of how this looks in the Diploma Supplement is shown in Figure 6.

Figure 6: Sample Recognition of Profile Preparation Based on Recommended Modules, for a Student Who Chose the Cyber Legal Pathway.



3.8 Joint Degree Award and Legal Recognition

Upon successful completion of the programme, you will be awarded a **Joint Master's Degree**, officially recognised under European regulations. This degree is jointly conferred by the three awarding universities:

- **UDS** – German University of Digital Science (Germany).
- **MTU** – Munster Technological University (Ireland).
- **UNIR** – Universidad Internacional de La Rioja (Spain).

Your joint diploma carries full legal recognition in Germany, Ireland, and Spain. It is also recognised across the **European Higher Education Area (EHEA)** through alignment with the **European Qualifications Framework (EQF, Level 7: master's)** and is widely accepted internationally.

3.8.1 Documents You Receive upon Graduation

You will receive two official documents upon graduation:

1. **Joint Degree Certificate**
   This diploma confirms the completion of 60 ECTS credits and the award of the academic title:
   "**Master of Science in Cybersecurity Management and Data Sovereignty**."
   It is jointly signed and certified by UDS, MTU, and UNIR.

2. **Joint Diploma Supplement**
   The Diploma Supplement provides transparent and standardised documentation of your academic achievements, including:
   - A full list of completed modules, ECTS credits earned, and percentage points (grades) achieved.
   - Grade interpretation tables and explanations of the academic systems in Germany, Ireland, and Spain.
   - A description of the programme structure and learning outcomes.
   - Recognition of your selected professional profile, if applicable.

- Documentation of your individual learning pathway, including your thesis topic.
- Official extracurricular engagement, such as service as a student representative.

Both documents are issued in English and fully comply with standards set by the European Commission, Council of Europe, and UNESCO/CEPES, ensuring transparency and international recognition.

3.8.2 Transcripts and Recognition of Credits

As a **Joint Master's Programme**, your academic progress is recognised seamlessly across all three awarding universities. No matter where a module is delivered or assessed, the **ECTS credits** you earn are **automatically recognised** by UDS, MTU, and UNIR.

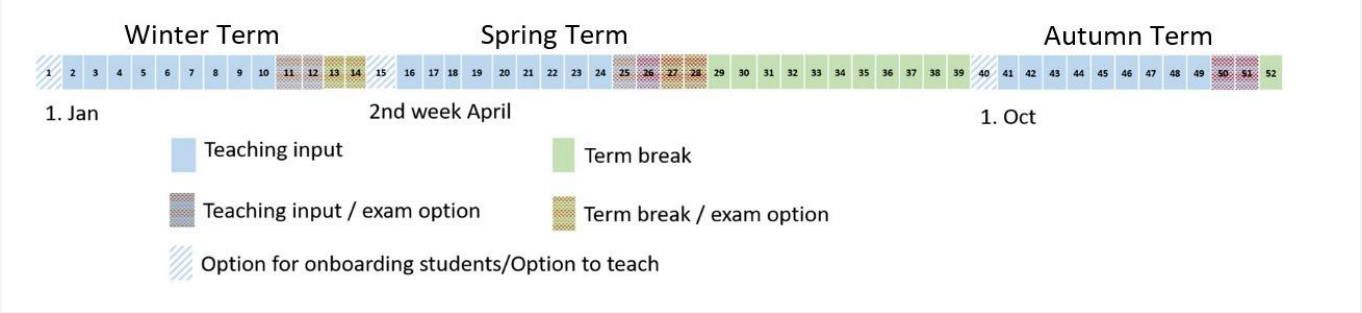
All awarded credits are recorded in a **centralised student record system** within the **Digital4Security platform** (explained in Section 14), ensuring transparency, fairness, and full academic continuity throughout your studies.

You may request an official **Transcript of Records** at any point during or after the programme, providing formal documentation of your academic progress and achievements. The **Welcome Module** offers guidance on how to request your transcript on the learning platform.

3.9 Academic Calendar

The academic calendar for the 60 ECTS Online Master's Programme in Cybersecurity Management and Data Sovereignty is structured across **three terms (trimesters) per year**, as illustrated in Figure 7. Each term has a standard duration of 12 weeks.

Figure 7. The Academic Calendar Across the Weeks of the Year.



In the Winter and Spring Terms, lecturers may schedule final exams during the regular teaching period or in weeks 13 or 14. The Autumn Term comprises only 12 weeks, followed by the Winter/Christmas Break, so all examinations are completed within the teaching period.

The terms typically run as follows across the year:

- **Winter Term**: January to March.
- **Spring Term**: April to June.
- **Autumn Term**: October to December.

3.10 Institutional Calendars and Staff Availability

As a student in this joint degree programme, you are affiliated with three awarding universities across Europe: UDS (Germany), MTU (Ireland), and UNIR (Spain). While all modules within the joint programme are fully supported by lecturers during their scheduled delivery periods, it may be helpful to remember that **each institution operates on its own internal academic calendar**.

This means that, beyond the official calendar of the joint degree programme, some institution-specific services or responses to queries (e.g. from programme coordinators or support staff) may be subject to institutional holiday periods.

To help you plan your communications effectively, table 3 provides an overview of lecturer and staff availability across the partner institutions throughout the year. In this overview, the following colour-code is used:

- Green: Regular teaching term; full personnel availability.
- Orange: Institutional break; limited personnel availability.
- Red: Core holiday period; no availability expected.

Table 3: Lecturer and Staff Availability across the Awarding Partners.

	January				February				March				April				May				June			
	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4
UDS																								
MTU																								
UNIR																								

	July				August				September				October				November				December			
	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4
UDS																								
MTU																								
UNIR																								

In Spain, the holiday week around the beginning of April coincides with the annual Easter period and may vary slightly across the years.

3.11 Required Equipment and Recommendations

To successfully participate in this online study programme, learners need to ensure they have access to appropriate equipment and an environment that supports flexible, focused, and effective learning.

Essential Equipment:

- **Laptop or Desktop Computer:** A reliable computer capable of running video conferencing tools, accessing cloud-based learning platforms, and using

standard productivity software (e.g., word processing, spreadsheets, presentation tools).

- **Internet Connection:** A stable and sufficiently fast internet connection is essential for streaming lectures, participating in live seminars, and uploading assignments.
- **Webcam and Microphone:** Many interactive activities, including oral assessments and group discussions, require audio-visual participation. Most modern laptops already include these features; external webcams and microphones may improve quality.

Recommended Additional Tools:

- **Audio Player or Smartphone with Audio Playback Capabilities:** For flexible learning, students are encouraged to rehearse lecture audio files, or listen to podcasts recommended within the modules, during everyday activities such as walking, commuting, or doing chores, helping to integrate learning into daily routines.
- **External Storage or Cloud Backup:** To avoid data loss, students should regularly back up their work using external hard drives or cloud services (e.g., those provided via the Online Learning Platform).

Study Environment:

Learners are advised to establish a **dedicated study space** that allows for concentrated work. This ideally includes:

- A desk and comfortable chair to support a healthy and active posture and productivity.
- A quiet setting with minimal distractions.
- The ability to shut the door to mark clear boundaries for study time, especially during assessments.

At the same time, different environments can inspire creativity and support varied study preferences. Learners are encouraged to identify **additional settings** that suit their personal needs, such as:

- A garden, park or balcony for open-air learning in a nature-inspired setting.
- Cafés or libraries for ambient background activity.
- Co-working spaces to promote active focus and occasional social interaction with other professionals or learners.

Finding a balance between focus and flexible engagement can significantly enhance long-term dedication, well-being, and academic success throughout the programme. The **Welcome Module** provides further suggestions and ideas for inspiration.

4. Curriculum

The Joint Master's Programme in Cybersecurity Management and Data Sovereignty offers a 60 ECTS fully online degree that prepares you for leadership roles in cybersecurity. The curriculum is developed in line with the European Qualifications Framework (**EQF Level 7**: master's level) and draws on input from academic experts, employers, and regulatory bodies across Europe. It balances managerial, technical, and legal perspectives with a strong emphasis on flexibility, real-world relevance, and career development.

While this section offers a concise overview, the curriculum and learning outcomes are also explained through a video message in the **Welcome Module**. Additionally, the **Module Handbook** provides in-depth details.

4.1 What Is a Module?

In this degree programme, your studies are organised into **modules**. A module is a self-contained unit of learning focused on a specific topic, such as cybersecurity law, cloud infrastructure, or risk management. In everyday terms, you can think of it as the individual **course** you enrol in for a given term.

Each module includes a blend of **teaching materials, interactive activities, assessments**, and clearly defined **learning outcomes**. These are designed to help you gain specific skills and knowledge relevant to the field that is addressed.

Modules are associated with **ECTS** credits **(European Credit Transfer and Accumulation System)**. In this programme, each taught module carries **5 ECTS**, which equals approximately **125 hours of total student work** – covering lectures, readings, assignments, self-study, and exam preparation. The only exception is the **thesis module**, which carries **15 ECTS** and represents roughly **375 hours of work**.

The thesis may span more than one term. All other modules are completed within a single term: **Winter, Spring,** or **Autumn**.

Some modules are **mandatory** for all students, while others are **elective**, allowing you to tailor your learning journey. You may also follow a recommended set of electives aligned with a **professional profile** (Section 3.7), depending on your career goals.

In short, modules are the building blocks of your degree, and your future career.

4.2 The Module Guarantor System

This online master's programme is delivered through a unique collaboration between three degree-awarding universities and a wide network of specialist academic and industry partners from across Europe, united by the shared vision of the **Digital4Security (D4S) Project**.

Each module is supported by expert teaching staff, some from the degree-awarding universities, and others from the broader D4S academic network. This design allows you to benefit from a wide variety of academic, professional, and cultural perspectives on cybersecurity.

4.2.1 A Networked Learning Experience

The D4S network brings together institutions and lecturers from across many European countries, each contributing distinctive expertise, practices, and outlooks. As a student, you gain:

- **Exposure to leading experts** in diverse cybersecurity domains from across Europe;
- **First-hand insights into national and sectoral cybersecurity approaches** across different legal and regulatory environments;
- **The opportunity to learn with and from practitioners** handling real-world tools and addressing a wide range of cybersecurity challenges and domain-specific problems;

- **Access to innovative teaching styles and case studies** used by different partner institutions;
- **The chance to build relationships and professional networks** that support career mobility, research collaboration, and entry into high-impact European cybersecurity initiatives.

This networked approach allows you to forge connections with instructors and peers across institutions: connections that may support your professional growth, international mobility, future research collaborations, or even career opportunities in European cybersecurity initiatives and organisations.

4.2.2 Academic Accountability and Quality Assurance

At the same time, your learning experience is firmly supported by the degree-awarding universities. For every module, one of the awarding universities is designated as the **accountable institution** (or **Module Guarantor**). This institution takes full academic and operational responsibility for the module, even if the teaching is carried out by another partner.

The Module Guarantor is responsible for:

- Ensuring the module aligns with the overall programme learning outcomes;
- Confirming that the content supports achievement of the module's learning outcomes;
- Reviewing and approving learning materials and assessments;
- Monitoring the quality of teaching and delivery;
- Serving as an additional academic and administrative contact for the module, beyond the immediate lecturer(s);
- Providing teaching support if the delivering partner becomes unavailable.

4.3 What Are ECTS?

ECTS refers to the **European Credit Transfer and Accumulation System**. It was developed to make higher education qualifications more transparent and comparable across Europe.

Previously, each country had its own system for measuring academic progress, which made it difficult to understand or recognise study achievements from one country to another. ECTS solves this by offering a unified standard. It helps students, universities, and employers understand the volume and level of learning involved in a qualification – making it easier to move between institutions or countries and have your qualifications recognised. In short: ECTS help your degree travel across borders.

Here is how the **ECTS Users' Guide** explains the core idea:

> **ECTS credits** express the volume of learning based on the defined learning outcomes and their associated workload. 60 ECTS credits are allocated to the learning outcomes and associated workload of a full-time academic year [...].
>
> **Learning outcomes** are statements of what the individual knows, understands and is able to do on completion of a learning process. The achievement of learning outcomes must be assessed through procedures based on clear and transparent criteria [...].
>
> **Workload** is an estimation of the time the individual typically needs to complete all learning activities such as lectures, seminars, projects, practical work, work placements and individual study required to achieve the defined learning outcomes [...]. It should be recognised that this represents the typical workload and that for individual students the actual time to achieve the learning outcomes will vary.
>
> (European Union, 2015, p. 10)

For example, a student with prior experience in a subject area might complete some tasks faster than average. The ECTS workload estimate serves as a planning tool for a "typical learner."

If you are curious to read more, the European Commission has made the full **ECTS Users' Guide** available online. It is very accessible and may be worth a look:

> European Commission. (2015). *ECTS users' guide*. Publications Office of the European Union. Available for download.

4.4 Modules

This section provides you with a concise overview of the modules included in the study programme. For more detailed information, please consult the **Module Handbook**.

4.4.1 Mandatory Modules

The programme includes three mandatory taught modules that all students need to complete. Each awarding university delivers one of these core modules. Together, the mandatory modules account for a **total of 15 ECTS**.

The mandatory modules are:

- **Communication Design for Cybersecurity** (UDS, 5 ECTS)
- **Business Resilience, Incident Management, and Threat Response** (MTU, 5 ECTS)
- **Ethical Hacking and Penetration Testing** (UNIR, 5 ECTS)

These mandatory modules provide complementary core perspectives that are essential to the programme's overarching focus on cybersecurity management and data sovereignty, particularly in the context of SMEs. The first module builds managerial competence through communication and compliant, strategic design skills (UDS). The second module delivers a business-oriented approach centred on organisational resilience (MTU). The third one offers critical technical depth in cybersecurity operations (UNIR). This structure ensures that all students, regardless

of their chosen professional pathway, acquire foundational knowledge across the programme's three defining content pillars.

Additionally, by completing one mandatory module at each of the three awarding universities, you will have actively studied at all institutions that co-sign your joint degree certificate by the end.

4.4.2 Recommended Modules for Professional Profiles

You have the option to align your studies with a **Professional Profile**, allowing you to follow a curated learning path tailored to a specific cybersecurity role. These pathways help guide your module selection based on career goals and industry demand, as defined by the **European Union Agency for Cybersecurity (ENISA)**.

Each pathway consists of a set of **recommended modules**, carefully selected to equip you with the core competencies needed for a particular professional role. Completing at least **15 ECTS** (3 modules à 5 ECTS) from the recommended modules of your chosen pathway qualifies you for formal recognition of that profile in your **Diploma Supplement** (cf. Sect 3.7).

Participation in a professional pathway is **optional**. If you prefer, you can freely select your elective modules without committing to a specific profile. However, choosing a pathway is highly recommended. It provides you with more focused support, clearer direction, and a credentialed advantage when entering or advancing in the job market. Below is a summary of the six professional pathways and their recommended modules:

Chief Information Security Officer (CISO) – curated by UDS
Focus: Leadership, governance, resilience, communication, and strategic decision-making.

- Cybersecurity Culture, Strategy & Leadership
- Law, Compliance, Governance, Policy, and Ethics

- Cybersecurity Economics & Supply Chain
- Risk Management of Cyber-Physical Systems
- CISO and Crisis Communication
- AI & Emerging Topics in Cybersecurity

Cybersecurity Educator – curated by UDS
Focus: Pedagogy, training delivery, research methods, and interdisciplinary understanding.

- Cybersecurity Education & Training Delivery I
- Cybersecurity Education & Training Delivery II
- Cybersecurity Culture, Strategy & Leadership
- Research Methods
- Law, Compliance, Governance, Policy, and Ethics
- AI & Emerging Topics in Cybersecurity

Cyber Legal, Policy, and Compliance Officer – curated by MTU
Focus: Legal frameworks, data sovereignty, ethics, governance, and compliance operations.

- Law, Compliance, Governance, Policy, and Ethics
- Cybersecurity Auditing
- Cybersecurity Law and Data Sovereignty
- AI & Emerging Topics in Cybersecurity
- Digital Forensics, Chain of Custody and eDiscovery

Cybersecurity Risk Manager – curated by MTU
Focus: Risk assessment, systems-level thinking, compliance, and crisis response.

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

Cyber Threat Intelligence Specialist – curated by UNIR
Focus: Offensive/defensive tactics, malware, threat detection, and data-driven analysis.

- Threat Intelligence
- Technological Foundations in CS & Security Controls
- Security Operations
- Automation of Security Tasks and Data Analytics
- Malware Analysis
- Enterprise Architecture, Infrastructure Design and Cloud Computing

Cybersecurity Auditor – curated by UNIR
Focus: Auditing practices, compliance, forensic readiness, and technical documentation.

- Cybersecurity Auditing
- Law, Compliance, Governance, Policy, and Ethics
- Cybersecurity Law and Data Sovereignty
- Risk Management of Cyber-Physical Systems
- Security Operations
- Digital Forensics, Chain of Custody and eDiscovery

4.4.3 The Module Catalogue

One of the distinguishing features of this joint master's programme is the **wide range of elective modules**, giving students the ability to tailor their studies to specific career goals, technical interests, or professional development needs. Beyond the three shared mandatory modules and the final thesis, students can select **six additional modules (30 ECTS)** from a diverse catalogue of specialised topics, spanning technical, managerial, legal, and educational domains of cybersecurity.

Out of the 30 ECTS of elective options, it is highly recommended that you choose 15 ECTS aligned with a professional profile (cf. sect. 4.3.2).

This structure enables you to **customise your learning journey**, focus on areas most relevant to your current role or future ambitions, and benefit from a truly interdisciplinary, multi-institutional learning experience.

Table 4 lists all the modules included in the **Module Handbook**.

Table 4: 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

No.	Module	ECTS	Programme Relation	Delivering Partner	Module Guarantor
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
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

No.	Module	ECTS	Programme Relation	Delivering Partner	Module Guarantor
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

You may notice that the **Welcome Module** is not included in the overview above. That is because it serves as an onboarding and communication tool. The Welcome Module does not carry ECTS credits, and it does not cover the programme's learning outcomes. However, it is available on the Learning Management System (LMS) alongside your other modules, providing practical guidance and support to help you start your studies smoothly.

While we are committed to offering a broad selection of elective options, **module availability may depend on student demand**. In particular, if overall enrolment numbers are low, the number of electives running in parallel may be reduced. To ensure a sustainable and high-quality learning experience, elective modules may furthermore be subject to **minimum enrolment thresholds**, for example, a minimum of five students need to register for a module for it to be launched in that term.

Mandatory modules, by contrast, are guaranteed to run regardless of enrolment numbers.

For students who opt into a **professional profile**, we guarantee that at least **four recommended profile-specific modules** will be delivered within the standard study duration (e.g., one year for full-time students). In addition, the programme ensures that **profile-specific academic support and learning pathways will remain**

available for at least five years following the student's initial selection of the profile at the point of admission.

4.4.4 Teaching and Learning Methods

This fully online degree programme is delivered using a blend of asynchronous and synchronous formats. Teaching methods may include:

- Pre-recorded lectures and digital learning resources
- Live webinars, problem-solving or Q&A sessions
- Case studies, design tasks, simulations, and practical exercises
- Peer feedback and team projects
- Portfolio work and project-based assessments

Each module includes guided learning tasks, self-study, and opportunities for formative feedback. You may also take part in online discussions, simulations, and reflective assignments. Scalable and flexible assessment formats ensure that the programme remains high-quality and learner-centred, even with a large international cohort.

You can find more detailed information on module-specific methods in the **Module Handbook**, while the **Study and Examination Regulations** cover more details on the permitted and recommended methods in this programme.

4.5 Understanding Programme-Level vs. Module-Level Learning Outcomes

In this Master's programme, learning outcomes are defined at two levels:

- **Programme-level learning outcomes** reflect the broader competencies and skills you should have mastered by the time you complete the entire degree.

- **Module-level learning outcomes** describe what you are expected to know, understand, and be able to do by the end of a specific module. These outcomes are directly linked to the content, assignments, and assessments of that individual course.

Each module is carefully designed to contribute to one or more of the broader programme-level outcomes. In other words, by completing individual modules, you progressively build toward fulfilling the overall goals of the programme.

The programme is consistently designed around a **60% point threshold** as the benchmark for minimum achievement, both at the **module level** and for the **programme as a whole** (Section 6.2 offers further detail). This means that when you successfully complete the required 60 ECTS – passing each module by achieving **at least 60% of the total available points** – you are considered to have fulfilled all intended **Minimum Learning Outcomes** of the programme.

These **Minimum Learning Outcomes** define the essential knowledge, skills, and competencies every graduate of the programme must demonstrate. While students are encouraged to aim higher, this threshold ensures a clear and fair standard of academic success and qualification.

4.6 Programme-Level Learning Outcomes

On successful completion of your studies, you will have gained advanced competencies in cybersecurity management and data sovereignty, comprising the abilities listed in Table 5.

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.

No.	Programme Learning Outcomes
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 to implement effective security operations, and to enable the proactive identification, assessment, and mitigation of cyber threats.
PLO6	Effectively apply analytical and strategic thinking 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.

4.7 Modules and their Relation to Programme-Learning Outcomes

Each module is carefully designed to contribute to one or more of the programme-level learning outcomes. Table 6 provides an overview of how each module supports the programme-level learning outcomes through their specific module-level topics.

Table 6: Modules Mapped to Programme 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
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

5. Admission and Enrolment

This section offers a concise overview of the requirements and procedures when you apply to the master's programme and complete your enrolment.

Additional guidance is available in the **Welcome Module**.

For full details on admission and enrolment, please consult the **Study and Examination Regulations**. Guidance on where to find these programme resources is provided by the end of this document.

5.1 Admission Requirements

To be eligible for admission, applicants must meet the following minimum requirements:

- A **Bachelor's degree** in any discipline (EQF Level 6 or national equivalent) from an accredited higher education institution;
- **English language proficiency** at minimum **CEFR level B2**.

In addition, applicants must have sufficient basic technological infrastructure to successfully participate in a fully online programme, such as a laptop and a reliable internet connection. By successfully completing the online application process, you demonstrate that you meet this requirement. As part of your Student Agreement, you also acknowledge that these technical conditions will be necessary throughout your studies and confirm that you will ensure ongoing availability.

Although the formal entry requirement for this master's programme is a bachelor's degree in any field, the programme is particularly suited for applicants with a background in at least one of the following domains:

business, compliance, (risk) management, law, public administration, computer science, data science, engineering, or other **numeracy-related disciplines**.

If you are unsure whether your background aligns well with the programme's content, we encourage you to reach out to the admissions team at t✉@ online.admissions@digital4security.eu for guidance.

5.2 Demonstrating Your Language Proficiency

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, or an official email, stating the applicant's role, period of employment, and that English was used as the primary language 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 7.

Table 7: 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

5.3 Enrolment Process

Once admitted, your formal enrolment will be coordinated through the **Digital4Security** platform.

After signing the **Learning Agreement** and paying the **participation fee**, your enrolment will be completed.

You will then receive your **access credentials** along with institutional onboarding guidance. This includes access to the **Welcome Module**, where you will find helpful resources and video guidance to support you as you begin your studies.

For questions from admission to formal enrolment, you can contact
online.admissions@digital4security.eu for further guidance.

Once you are formally enrolled, you can contact
studyaffairs@digital4security.eu for additional onboarding support.

5.3.1 Student ID and Access Rights

After enrolment, you will receive a **student identification number** from the Digital4Security platform.

The awarding universities may also assign you dedicated IDs in their systems, if required for accessing institutional resources.

5.3.2 Fee Payment, EU Co-Funding, and Country-Specific Considerations

Tuition fees for the 60 ECTS Online Master's Programme are centrally managed through the **Digital4Security platform**, which also serves as the main administrative contact point for billing and receipts. Upon enrolment, you will receive an official **payment schedule** and **receipt of payment**.

Fees can be paid **in full or in instalments**, depending on your preference.

Please note that tuition rates may vary depending on your chosen study track. For example, the 1-year full-time track may differ in price from the 2-year part-time track, as the latter incurs longer access to licensed tools and services. Switching between tracks (see Section 3) may result in an adjustment to your payment plan. Respective costs will be communicated transparently on the platform before you request or confirm a change of your study track.

The programme is designed to be inclusive and affordable, offering top-tier academic and professional training at a competitive cost. As part of an **EU co-funded initiative**, students benefit from substantial financial support:

- **All students**, regardless of location, benefit from high-quality instruction by leading European cybersecurity experts at a competitive, economic price.

- **EU/EEA students**, in particular, benefit from a **50% tuition reduction** thanks to EU co-funding. This discount is guaranteed for all European students **until 30 September 2027**, after which standard tuition fees will apply. *The prices displayed on the Digital4Security website, separately for European and non-European applicants, represent the final amounts, with any applicable reductions already included.*

Please also take into account **country-specific considerations**, which may affect your personal financial planning:

- In some countries, **tuition fees may be tax-deductible**
- **Student insurance requirements** (e.g., health insurance in your country of residence or any country you may visit)
- You may be eligible for **national funding schemes** or **Erasmus+ mobility grants.**

5.4 Recognition of ECTS from Microcredentials

In line with the Digital4Security's **stackable learning philosophy**, recognition of ECTS earned via microcredentials and microdegrees is possible as part of your 60 ECTS study load.

A **microcredential or microdegree** is a short, targeted learning experience that certifies specific competencies. If you have completed such credentials associated with ECTS credits in the field of Cybersecurity Management and Data Sovereignty, they may be eligible for recognition within your master's degree programme.

In this online Master's programme, up to 9 ECTS may theoretically be recognised from prior microcredentials, in line with European and national regulations. The upper limit reflects Spain's *Real Decreto 822/2021*, which allows recognition of prior learning for **up to 15%** of the total programme credits. However, since the Master's Programme does not include modules of 9 or 4 ECTS, in practice this

means that only **5 ECTS can be recognised through microcredentials**. Effectively, this allows you to replace exactly one elective module with a microcredential.

Notably, this microcredential may also be a module from the Master's Programme itself. This offers a unique opportunity: You can experience the programme before fully enrolling, by taking a module as a microcredential learner. If you enjoy the experience, you can then apply for the full Master's. Upon admission, the completed module will be recognised, and you will only need to complete the remaining 55 ECTS. This is a very special case, even allowing you to replace a mandatory module with a microcredential – but only if you have actually completed one of the mandatory modules of the 60 ECTS Master's Programme as a microcredential learner. In all other cases, recognised microcredentials count towards elective study options in the **Diploma Supplement**.

If you already hold relevant microcredentials at the time of your application, you can request recognition by completing the **microcredential recognition form** during the admissions process.

If you complete a qualifying microcredential after enrolment or wish to apply for recognition at a later stage, you can still do so **by contacting** secretariat@digital4security.eu. *Please note: This application for recognition is possible only* ***during the first two weeks of any running term****, as long as you are still enrolled, i.e. before completing your studies.*

ECTS will be **automatically recognised** if your micro credential was selected from the **Digital4Security platform**, referring to educational offerings associated with the programme. All such certificates issued by D4S will be recognised based on their assigned ECTS value.

Certificates aligned with the **European Digital Credentials for Learning (EDCI) standard** will be recognised according to their stated ECTS, provided that the microcredential's topics sufficiently align with the master's programme content and its learning outcomes.

Other credential formats – such as nationally accredited programmes or open badges – will be considered individually, subject to academic review and formal approval by the Examinations Board.

This recognition procedure is formally defined in the **Study and Examination Regulations**. Further guidance is also provided in the **Welcome Module**.

5.5 Re-Enrolling in the Programme and Recognition of Completed ECTS Credits

We understand that life circumstances can change, and you may need to pause your studies before completing your degree. If you have previously earned ECTS credits in this master's programme but had to withdraw before finishing, we warmly welcome your return.

5.5.1 Re-Enrolment: Your Pathway Back

If you choose to re-enrol in the programme later, you will be given **priority in the admissions process**. If there are no substantial academic or regulatory obstacles, you retain the **right to re-enter with full recognition of the modules you successfully completed** during your earlier studies.

5.5.2 What to Expect Upon Re-Enrolment

When you return:

- **Your previously earned ECTS credits will be fully recognised**, if they still align with the current curriculum and learning outcomes.
- Your re-enrolment will be governed by the **terms, conditions, fee structure, and academic regulations that apply at the time of your return**.

If the programme structure has remained unchanged, our administrative team can usually recognise your previous credits automatically. However, if the curriculum has been updated – especially through reaccreditation – the Admissions Board will carefully review your completed modules and confirm which ones can still count toward your degree. In more complex situations, they may consult with the Examinations Board to ensure a fair decision.

5.5.3 Important Considerations

Re-enrolment is only possible if you are eligible to complete the programme under the current regulations. Please note:

- If you previously **failed a required module or assessment the maximum number of times allowed**, you cannot be re-admitted (unless the programme has since been altered through reaccreditation and that module is no longer compulsory).
- If you were **expelled for serious academic misconduct**, you no longer have an automatic right to re-join the programme. In rare cases, the Admissions Board may recommend re-admission, but this would require approval by the Master's Board and a strong justification, such as proof of a procedural error or an unjust accusation that led to the original expulsion.

5.5.4 Thinking about Withdrawing?

If you are considering to withdraw from the programme, we strongly encourage you to reflect carefully and, if possible, speak with an academic advisor before making a final decision. While re-enrolment is an option, it's important to know that programme structures and requirements can change over time. This means some of your previously completed modules might no longer be compatible, or new mandatory components could be introduced. Only continuous enrolment guarantees that you can complete your degree under the same terms, conditions, and curriculum that were in place when you were first admitted.

You are welcome to contact **studyaffairs@digital4security** for confidential guidance and support. The team is here to help you make sense of your situation, appraise all options realistically, and take well-informed decisions.

6. Assessment

Assessment in the Joint Master's Programme is designed to ensure fairness, transparency, and academic integrity while supporting flexible learning and real-world application. The structure blends proctored summative evaluations with continuous assessment to reflect both academic mastery and professional growth.

This section offers a quick overview. For full details, please refer to the **Study and Examination Regulations**. To help you get started, the **Welcome Module** also includes short video explainers that walk you through the key rules and procedures.

6.1 Assessment Methods

Each module assigns at least 60% of the final grade to proctored or verified assessments and up to 40% to continuous assessment.

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.

Proctored assessments may include:

- Online exams using GDPR-compliant tools like SMOWL, which verify student identity and ensure only permitted resources are used during the exam (e.g., no colleague present telling the test-taker what to write)
- Live oral presentations with identity verification
- Employer-verified workplace projects

Continuous assessment may involve:

- Weekly learning tasks or case-based analyses
- Quizzes, reflection logs, or portfolios,

- Options to apply theory or methods to your professional context, or to choose between task domains (e.g. focussing on legal, managerial, or technical details in an overall task domain)
- Teamwork projects – peer reviewed and/or instructor reviewed

6.2 Grading Scheme

Your performance is assessed on a percentage basis and aligned with the joint grading scheme used throughout the master's programme. This scheme ensures consistency across all partner institutions and reflects how grades are interpreted within the programme.

Table 8 provides an overview of achievement classifications and their meaning in the master's programme.

Table 8: Joint Grade Classification

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

Grades are mutually recognised across institutions. The percentage grade is the official reference throughout the programme, and in the **Diploma Supplement**.

In addition, your results are translated into the national grading systems of Germany, Ireland, and Spain (see Table 9). The **Diploma Supplement** also provides an

overview of each country's educational systems. This conversion can be useful when applying for jobs or further studies in one of the partner countries, as it helps employers and institutions understand your achievements in locally familiar terms.

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)

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.

6.3 Late Submissions

Staying on track with deadlines is an important part of academic life. It ensures fairness for all and helps you build strong time management skills for your future career. All assignments and assessments are expected to be submitted by the published deadlines.

That said, we understand that life does not always go as planned. In cases of **exceptional and well-documented circumstances**, late submissions may be accepted. These include situations such as:

- Serious illness or scheduled medical procedures (e.g., surgery)
- Bereavement (loss of a close family member)
- Natural disasters or major emergencies that affect your ability to study or submit work
- Other significant, unforeseen events beyond your control

If you find yourself in such a situation, please reach out to your course instructor(s) **as early as possible**. With appropriate documentation, like a medical certificate, we can explore reasonable extensions or alternative arrangements on a case-by-case basis.

Please note: Deadlines related to work, travel, or general workload pressures are not considered valid reasons for late submission. We encourage you to plan ahead and seek support early if you are struggling to keep up.

By being proactive and transparent, you help maintain a positive learning environment, for yourself and your peers. And remember: If you are ever unsure about options or need advice, your instructors, the Programme Coordinator of your chosen professional profile, and the study affairs team are here to help.

- **Contact your course instructor** directly if you are unable to meet a submission deadline for a specific module. With valid documentation (e.g., a medical certificate), instructors can assess whether a short extension or alternative arrangement is possible.
- **Contact your Programme Coordinator** with the relevant instructors in Cc if your challenge affects multiple modules, for instance if you fell victim to a natural catastrophe and foreseeably will not be able to complete any module tasks within the next week.
- **Contact the study affairs team** at **studyaffairs@digital4security.eu** if your concerns are more general, such as falling behind across multiple modules, needing help with time management, or considering whether to switch tracks, e.g., from full-time to part-time. The team can help you explore realistic options to stay on track. Additionally, contact this team if you consider stepping down from one or more modules, particularly if you need clarification on how such changes would affect your overall study plan.

6.4 Exam Attempts

In line with the **Study and Examination Regulations**, modules offer two examination options, referred to as "calls":

- **Ordinary Call**: This refers to the primary (regular) examination session at the end of the module. All students are expected to take their final exam during this session.
- **Extraordinary Call**: This is a second and final opportunity to take the exam, available to students who did not pass the ordinary exam or could not attend that session. If no student falls into either category, this call is omitted.

The extraordinary call typically covers the same scope as the ordinary examination. Course instructors will provide details as needed. Module-specific regulations covering repeated examinations are included in the **Module Handbook**.

An overview and explanation of the examination procedure is also offered in a video within the **Welcome Module**.

6.5 Number of Exam and Module Attempts

You are allowed **up to two exam attempts per module enrolment**: once in the ordinary call and once in the extraordinary call (see Section 6.4). If you do not pass the module after these two opportunities, you may choose to re-enrol in the module in a later term, taking a fresh attempt.

Re-enrolment is designed to support continued learning and mastery of the subject. When re-enrolling, you will complete all components of the module again. Work or grades from previous enrolments do not carry over. Each enrolment is treated as a full, new opportunity to achieve the intended learning outcomes.

Please note: *Each examination may be attempted a maximum of four times in total, including all attempts across repeated module enrolments.*

Students are strongly encouraged to keep track of their examination attempts, especially for mandatory modules, which must be successfully completed to obtain the master's degree.

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

Students who have successfully completed 30 or more ECTS may be eligible for a Postgraduate Certificate (see Section 1.3.2).

6.6 Academic Integrity

Integrity is a core value of this programme and a foundation for your academic and professional growth. Upholding academic integrity means producing original work, giving proper credit to the ideas of others, and engaging honestly in all forms of assessment.

Detailed guidance on this subject is provided in the **Study and Examination Regulations**, while this section offers a concise overview. You may also explore the **Welcome Module** materials, which include tailored training, resources, and helpful pointers.
To support a fair and transparent learning environment, the programme uses a range of measures, including:

- Proctored exams
- Plagiarism checks
- Clear authorship expectations
- Transparent assessment documentation, including rubrics and grading criteria made available in advance through the learning platform

If academic misconduct is suspected, the case will be reviewed thoroughly. Students will always have the opportunity to respond and explain their situation before any decision is made. The goal is not only to maintain high academic standards, but also to support learning and improvement.

Students are strongly encouraged to take an active role in reviewing their own work. Tools that offer plagiarism checks, like Turnitin, can be used not just for formal reviews, but also as learning resources to:

- Identify missing or incomplete citations
- Improve referencing and paraphrasing
- Reflect on how sources are used and integrated
- Strengthen academic writing practices over time

Using these tools proactively can help you grow as a writer, researcher, and future professional.

This master's programme is designed to help you develop strong academic and professional competencies, including how to work with sources responsibly. In the **Welcome Module**, you receive guidance on how to reference materials professionally in academic contexts, whether you are citing human authors or content generated by AI tools.

In the case of **AI-generated content**, please pay close attention to the specific expectations outlined by your lecturers for each assessment. The programme supports the development of ethical AI literacy, recognising it as a key skill for professionals in Cybersecurity Management and Data Sovereignty. However, it is essential to follow the rules provided for each assignment. Lecturers will specify whether and how AI tools may or may not be used.

In all cases, **transparent and proper referencing is required**. This ensures academic integrity and helps you build the skills needed for responsible knowledge work in both academic and professional settings. Overall, upholding integrity is not just about following rules. It is about developing your voice and confidence as an ethical contributor in your field.

7. Programme Governance

The **Joint Master's in Cybersecurity Management and Data Sovereignty** is governed through a collaborative structure that ensures high academic quality, fair decision-making, and a strong student focus across all partner institutions. Each awarding university – UDS, MTU and UNIR – plays an active role in programme management, quality assurance, and student support.

This section provides a brief overview of the programme's management structure, as defined by the **Cooperation Agreement** between the partner institutions. It is intended to help you better understand the framework of your studies: introducing key governance bodies you may encounter (such as the Examinations Board) and professional roles that are relevant for you (such as the Programme Coordinators you can contact for support). Additional guidance is available in the **Welcome Module**, including a video explaining the governance structure.

7.1 Key Roles and Responsibilities

Programme Directors
Each of the three awarding universities appoints a Programme Director who is responsible for ensuring that the programme runs smoothly at their institution. Together, they coordinate the academic integrity and strategic development of the joint degree.

Programme Coordinators
Programme Coordinators assist with day-to-day administration, student support, virtual mobility, and quality assurance. They are your first point of contact for operational matters and work closely with the Secretariat and fellow Coordinators across institutions.

Programme Faculty
Academic staff from partner universities and associated institutions contribute to teaching, project-work, assessment, and mentoring. Their varied backgrounds ensure interdisciplinary and international perspectives.

Coordinating Institution (UDS)
UDS acts as the coordinating university for this joint degree. It oversees the implementation of core operations such as admission and enrolment, student onboarding, the continued availability of the learning platform and tools, student services, industry certifications, and employability support. UDS also leads efforts to ensure the programme's long-term sustainability and institutional integration beyond EU funding.

7.2 Governance Bodies

The governance of the programme is supported by several joint bodies, as introduced below. These are in place to ensure transparent, inclusive, and quality-driven decisions across institutions.

Master's Board of Directors
This is the programme's highest decision-making body. It includes the Programme Directors of UDS, MTU, and UNIR, as well as a Council Representative from UDS providing strategic guidance on long-term institutional sustainability. The Board holds full authority over all decisions related to the joint degree programme, ranging from academic governance and quality assurance to programme development and appeals. All decisions require a two-thirds majority.

Programme Secretariat
Hosted at UDS, the Secretariat handles the day-to-day operations of the programme, such as admissions and enrolment, quality assurance outreach, student service provision, IT helpdesk support, the coordination of student mobility, and where applicable support for student clubs and student life activities. It also assists the Master's Board and other governance bodies.

Joint Admissions Board
This board is responsible for selecting and admitting students. It consists of one representative from each awarding university and is supported by the Secretariat.

Examinations Board
Chaired by the Master's Board, this body ensures academic integrity and fairness across all assessments. It monitors exam procedures, reviews results, and upholds the jointly agreed assessment standards.

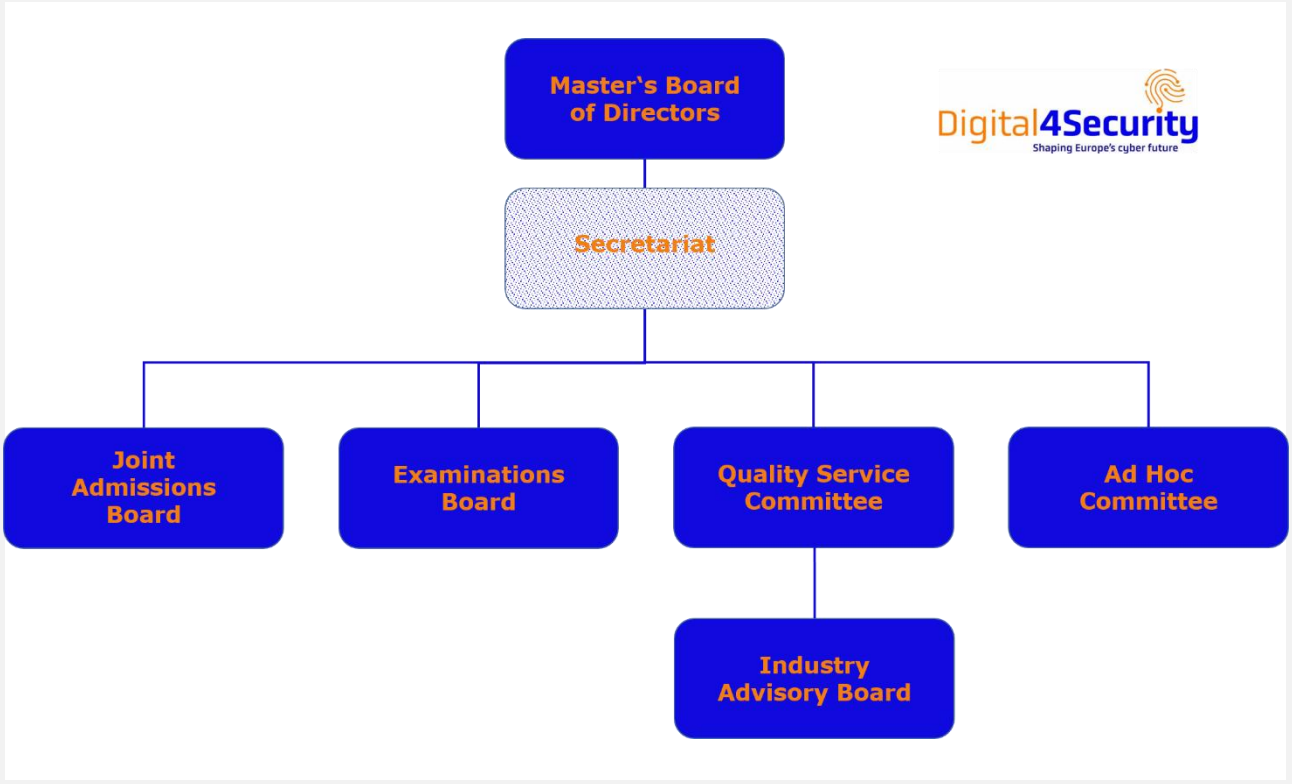
Quality Service Committee
This body supports curriculum development and continuous programme improvement. It reviews student feedback, academic performance data, and input from relevant stakeholders. The committee contributes to strategic planning and fosters innovation in a student-centred and industry-aligned manner. It also prepares the draft of the **Annual Programme Review Report**, which serves as a key source of data, insights, and recommendations for programme enhancement. The committee includes two student representatives, at least one faculty member from each awarding university, one representative from the Secretariat, and up to three industry experts.

Industry Advisory Board (IAB)
The IAB is an external group of cybersecurity professionals from the Digital4Security network. It provides independent advice to ensure the programme remains aligned with evolving industry needs, especially in SMEs. While it does not make formal decisions, its recommendations influence curriculum updates and practical learning components.

Ad-hoc Committees
Temporary committees may be created to address specific tasks or emerging topics. These are formed by the Master's Board as needed, while they can also be recommended by the other governing bodies.

An overview of the governance structure is presented in Figure 8.

Figure 8: Governance Structure of the 60 ECTS Online Master's Programme.



As Figure 8 illustrates, the highest decision-making authority rests with the Master's Board. The Secretariat supports day-to-day operations and assists various boards and committees. The Industry Advisory Board operates largely independently from the Master's Board, acting as an "external corrective" to ensure continuous industry alignment by providing data and recommendations to the Quality Service Committee.

8. Student Representative Election

This Master's programme embraces a **student-centred approach**, following a **university-as-a-service model**. As part of this vision, students are strongly encouraged to actively shape the university culture, promoting collaboration, mutual support, and continuous improvement. Student representatives play a central role in this process.

8.1 Roles of Student Representatives

Student representatives contribute both formally and informally across a range of activities. Some official roles include:

- Serving as **voting members in the Quality Service Committee**, which monitors student satisfaction and learning outcomes, while also recommending innovative improvements.
- **Co-organising the Future of Learning Convention**, an annual event where students, faculty, management, alumni, and industry representatives reflect on the programme and its relevance for evolving professional and academic fields, gathering ideas for improvement.
- Participating as **invited (non-voting) guests in meetings of the Master's Board**, where they may contribute in an advisory capacity.
- Acting as **points of contact for student feedback or concerns**, as part of the "I Wish, I Like, and Clarify" process outlined in the **Internal Quality Handbook**.

In addition, student representatives may take on informal or self-organised roles, such as:

- Participating in **thematic working groups** (e.g. for diversity, platform usability, onboarding, etc.).

- Supporting **student clubs**, peer mentoring, or **social events** within the learners' community.
- Acting as **regional or pathway-specific contact persons** (e.g. for part-time learners or specific professional profiles).
- **Gathering and communicating feedback** across intakes and student cohorts.
- Helping to **build community** across the three awarding universities and the large international network of partners.

8.2 Purposes of Representation

The aims of student elections include:

- **To empower the student voice** within a learning environment committed to a student-centred approach and the university-as-a-service model.
- **To ensure fair representation** across a growing and diverse student body, reflecting the variety of backgrounds, learning pathways, and lived experiences within the programme.
- **To promote democratic legitimacy and inclusion** in the governance and ongoing development of the joint programme.

8.3 Number of Student Representatives

The number of elected student representatives shall be proportionate to the size of the student body, with upper and lower bounds.

One representative shall be elected per 100 students, with one additional representative for each additional 100 students.

A **maximum of 10 representatives shall be elected** if the student body exceeds 1000 students.

There shall be **no fewer than two elected student representatives**, even if the total number of enrolled students is below 100. This ensures the required minimum representation on the **Quality Service Committee**.

8.4. Organisation of Elections

The election process is organised by the Programme Coordinators. They are responsible for:

- Issuing the call for nominations
- Communicating procedures and timelines
- Overseeing the voting process
- Announcing the results

8.5. Scope of Student Representation

Student representatives serve as liaisons between the student body and programme leadership. Their responsibilities include:

- Gathering and relaying student feedback
- Participating in meetings and quality review processes
- Contributing to the continuous improvement of the student experience
- Supporting community-building and peer networking initiatives

8.6 Election Process

8.6.1 Timing

Elections are ordinarily held **twice per year**, shortly after the Welcome Week of each intake.

In case of a vacancy or mismatch between student numbers and representative slots, additional elections may be held, or the Programme Coordinators may appoint the next eligible candidate(s) from the previous election.

Elections are held over one week.

Each cohort ordinarily participates in one election per year, typically after their Welcome Week. Elections are conducted jointly across the student body, rather than separately by cohort. This ensures fair competition for available seats and integration across intakes.

As student numbers grow and new representative seats become available, elections shall, where possible, be distributed across the year, with the aim of ensuring that both annual intake cohorts have the opportunity to vote for approximately equal numbers of seats.

If no representative seats are available at the time of a cohort's scheduled election, the cohort retains the right to vote in the next election where seats become available. This serves to ensure that all student groups have a fair opportunity to participate in shaping representation over time.

8.6.2 Eligibility

All currently enrolled students may:

- Nominate themselves
- Nominate others
- Vote in the election

8.6.3 Voting Method

Voting is conducted anonymously and online, using a secure platform selected by the Programme Coordinators.

8.6.4 Voting Procedure

Elections are decided by majority vote. Students may vote for as many candidates as there are open positions. The candidates with the highest number of votes are elected.

8.6.5 Tie-Breaking Procedure

In the event of a tie:

- If only one candidate is a full-time student, that candidate wins.
- If still unresolved, the winner is selected by random draw conducted by the Programme Coordinators.

8.7 Term Length

Student representatives serve a term of 12 months, or until they complete their studies, withdraw from the programme, or resign from their role - whichever comes first.

8.8 Re-election and Replacement

Representatives may be re-elected for consecutive terms.

If a representative resigns or becomes inactive, they may be replaced according to the same procedures, or by appointing the next-ranked candidate from the previous election. The Programme Coordinators are responsible for handling vacant seats in such a way as to maximize the chances of all cohorts for fair and timely representation.

If a next-ranked candidate is appointed without a new election, they shall serve only for the remainder of the original representative's term, completing the originally allotted 12-month period. If the replacement is elected through a new election, they may serve a full term of up to 12 months, as specified in Section 8.7 on Term Length.

If a student representative becomes inactive – for example, by not responding to communications or missing key meetings without notification or excuse – the Programme Coordinators may initiate a replacement process. Before doing so, the representative will receive a written notice and a two-week period to respond or resume their duties.

If no response is received or the representative confirms their withdrawal, the position may be filled either through:

- **The next-ranked candidate** from the previous election, or
- **A new election**.

This ensures that students continue to have active and reliable representation throughout the academic year.

8.9 Recognition in the Diploma Supplement

If you are elected and serve as a student representative, your contribution will be **formally recognised in your Diploma Supplement**, under the section detailing additional qualifications and extracurricular activities. This recognition highlights your leadership role, participation in academic governance, and your contribution to shaping the learning experience of your peers.

9. Student Rights and Responsibilities

As a student in this master's programme, you are part of a diverse, international academic community that values mutual respect, integrity, and excellence. This section outlines your rights and responsibilities throughout your studies. The **Welcome Module** also offers a video dedicated to this topic.

9.1 Code of Conduct

All students are expected to uphold high standards of **academic integrity**, **professional conduct**, and a **collaborative spirit**. This includes avoiding plagiarism, respecting intellectual property, and engaging in fair, transparent communication with peers, instructors, and staff. Dishonest behaviour in assessments or misrepresentation of work may result in disciplinary action.

You are encouraged to contribute actively and constructively to online discussions, team assignments, and live sessions. Respectful, inclusive behaviour is always expected.

Further information on academic integrity, particularly regarding assessments and submissions, can be found in Section 6.6 above. A detailed explanation is also included in the **Study and Examination Regulations**.

9.2 Equal Opportunities, Inclusion, and Diversity

The programme is committed to **equality, inclusion, and non-discrimination**. Students of all backgrounds – regardless of nationality, ethnicity, gender identity, age, disability, religion, or socioeconomic status – are welcomed and supported.

If you have specific learning needs, physical impairments, or face structural barriers to participation, please contact the support team at

studyaffairs@digital4security.eu

early in your studies, ideally upon registration. **Reasonable accommodations** can be arranged to ensure equal access to learning and assessment opportunities. Support will be considered on a case-by-case basis, taking into account the specific needs, and feasibility within the programme. Where appropriate, the study affairs team may also consult the Examinations Board to help identify viable solutions.

9.3 Student Feedback

Students play an active role in shaping and improving the programme. Your feedback is welcomed and gathered through:

- Module evaluations and programme surveys
- Student representation in programme coordination meetings
- Open feedback opportunities on the platform
- Optional focus groups
- Participation in the annual Future of Learning Convention: an event to discuss student experiences and to generate innovative ideas for the future
- Self-organized initiatives by the student body, i.e., via the student representatives

You are encouraged to contribute suggestions and help improve teaching, services, and content delivery. This continuous feedback cycle is part of the programme's **internal quality assurance**, as further described in Section 11 below**.**

9.4 Student Obligations

As a student, you are expected to:

- Engage actively with course content and collaborative activities
- Meet submission deadlines and adhere to academic schedules
- Participate in assessments honestly and independently
- Use the digital platform regularly and respond to communication from instructors and staff
- Inform the support team (**studyaffairs@digital4security.eu**) in case of extended absences or personal circumstances affecting your studies

While attendance at live sessions is usually not mandatory throughout the teaching period, regular participation in asynchronous activities is essential to academic progress.

Live attendance is required for certain assessments and examinations, which may also be subject to additional proctoring requirements (see Section 6). This includes identity verification procedures and measures to ensure that only permitted tools and methods are used. Compliance with these requirements is mandatory for participation in the programme, with your consent established through the Student Agreement signed upon admission.

9.5 Using Digital Platforms and Resources Responsibly

As a student in this master's programme, you have access to a wide range of digital platforms, communication tools, and learning resources. Using these tools responsibly is about fairness, respect, and collaboration. By engaging considerately, protecting confidentiality, and supporting your peers, you help create a learning environment where everyone can thrive. This is also part of developing the mindset of a cybersecurity professional: ethical, accountable, and ready to face the challenges of a complex digital world.

9.5.1 Digital Etiquette (Netiquette)

Learning online works best when everyone participates actively and considerately. Here are some simple ways to make your presence felt, and to support your peers:

- **Switch on your camera when possible** – it helps others feel connected and prevents speaking into a void.
- **Contribute to discussions** via audio or chat, sharing your ideas, questions, and experiences.
- **Be respectful and constructive** – consider different perspectives and help create an inclusive atmosphere.
- **Listen as well as speak** – engagement is a two-way street, and collaboration benefits everyone.

Small actions like these help create a learning environment where everyone can thrive.

9.5.2 Confidentiality of Assessment Materials and Individual Answers

Assessment materials – whether assignments, case studies, or exams – are provided for **your learning and completion only**. They are designed to help you demonstrate your understanding and develop your skills. To ensure fairness for all students, these materials shall **not be copied, shared, or circulated**, either physically or digitally, inside or outside the programme.

Similarly, your own submissions and those of your peers are confidential. Sharing your work results, or using someone else's, undermines trust and fairness in the learning community. Every student deserves to have their effort recognised, and everyone benefits when achievements genuinely reflect their own work.

Think of it this way: respecting confidentiality and working independently is not just a requirement – it is part of being a responsible, ethical professional, and it protects the integrity of your learning journey and that of your peers.

That said, collaboration is encouraged when it is part of your learning:

- **Team projects:** Share materials within your assigned group to complete tasks together.
- **Work-based projects:** Discuss work with mentors or colleagues as foreseen in your Learning Agreement.
- **Thesis work:** Peer review and discussion are encouraged, but the final thesis must be your own work. Acknowledge others' contributions where appropriate.

9.5.3 Using Learning Materials Thoughtfully

All learning materials provided through the programme – such as lecture recordings, slides, and other resources – are intended solely for your use within the programme. They must not be reproduced, shared, or distributed, as doing so breaches both academic integrity and copyright law.

In some modules, you may also have access to the work of other students for peer review, feedback, or collaborative learning. These contributions remain the intellectual property of their authors, and likewise they must not be shared with others inside or outside the programme.

9.5.4 Protecting Safety Together

Should you ever encounter content that is harmful, offensive, or unsafe, whether in discussions or peer work, bring it to the attention of your instructor. Speaking up helps protect the learning community and ensures everyone can participate safely. If you are unsure how to proceed and want confidential guidance, you may also contact **studyaffairs@digital4security.eu**.

9.5.4 Protecting Yourself and the Learning Environment

Being responsible online also means looking after your own accounts and data. Use secure connections, protect your login credentials, and follow data protection guidance (including GDPR). Avoid actions that could disrupt learning, compromise security, or affect fairness.

9.6 Disciplinary Procedures

In case of suspected academic or behavioural misconduct, a formal review will be initiated. The procedures follow the principles of **fairness, proportionality, and the right to be heard**. Possible outcomes may include a written warning, a failed grade for the affected assignment or module, or – only in severe or repeated cases – temporary suspension or exclusion from the programme. Further details can be found in the **Study and Examination Regulations**.

10. Support Services: Here for You

As a student in the 60 ECTS Online Master's Programme in Cybersecurity Management and Data Sovereignty, you benefit from a broad range of services designed to support your **academic success, personal development, and professional growth**.

The **Coordinating Institution, UDS**, is primarily responsible for organizing and delivering student services, including access to learning resources, technical support, and virtual campus life. You can also take advantage of special opportunities through UDS institutions such as the E-College, D-College, and Research Centers.

At the same time, **academic advisory services are offered by all three awarding universities: UDS, MTU, and UNIR**. This ensures that you have access to personalized academic guidance, mentoring, and programme-related support no matter where your interests or challenges lie.

Additional resources are available through the **Digital4Security platform** and the wider **network of partner institutions**. This offers you the advantage of a connected, international learning environment with access to experts from across Europe. They bring a rich diversity of institutional backgrounds and perspectives, giving you exceptional opportunities for networking and collaboration.

We are here to support you at every step of your journey: academically, professionally, and personally.

10.1 Academic and Learning Support

Welcome Week: Onboarding Support and Resource Hub

Upon admission to the programme, you gain access to this onboarding resource hub, which provides a foundational part of the student support system in the

programme. Designed to help you get started, it offers essential tools, documents, guidance, and inspiration for your academic journey.

The module serves as a multi-functional support base, covering the following key areas:

- Digital and academic readiness
- Study habits and environments for successful online learning
- Community and student engagement
- Well-being
- Career and skills development

You can revisit the module at any time during your studies. Further details are provided in Section 15.

Responsible: UDS
Contact: **coordinator.uds@digital4security.eu**

Academic Supervision and Advising

The three awarding universities – UDS, MTU, and UNIR – work together to ensure high-quality academic support throughout your studies. While each university offers broad cybersecurity expertise, their academic advising responsibilities are coordinated to match their strengths. These are reflected in both the mandatory modules they teach and the professional pathways they curate.

This means that depending on your area of interest as reflected in the professional profile you have chosen, you will benefit from targeted guidance by experts in that field, while still having access to cross-institutional support if needed.

German University of Digital Science (UDS)

Core Focus: Cybersecurity Strategy, Leadership, Innovation, and Education
UDS leads advising in areas related to **human-centred design, digital governance and innovation**, as well as **education in cybersecurity**. This reflects its responsibility for the mandatory module "*Communication Design for Cybersecurity*," which builds managerial competence and strategic communication skills essential to governance and leadership roles.

Curated Pathways:

- Chief Information Security Officer (CISO)
- Cybersecurity Educator

Advising Themes:

- Leadership and innovation, organisational culture, and crisis communication
- Compliance, ethics, and governance frameworks
- Research methods and digital education strategies
- Strategic transformation and stakeholder engagement

Students without a selected professional pathway may contact UDS for general academic support.

Munster Technological University (MTU)

Core Focus: Organisational and Industy Resilience, Risk Management, and Policy

MTU delivers the mandatory module "*Business Resilience, Incident Management, and Threat Response*," reinforcing its focus on **systems-level preparedness**, **policy integration**, and **risk-based decision-making** in cybersecurity.

Curated Pathways:

- Cyber Legal, Policy, and Compliance Officer
- Cybersecurity Risk Manager

Advising Themes:

- Legal frameworks and cybersecurity policy
- Risk assessment and regulatory compliance
- Operational governance and industry resilience
- Supply chain and business continuity planning

Universidad Internacional de La Rioja (UNIR)

Core Focus: Cybersecurity Operations, Threat Intelligence, and Forensics

UNIR delivers the mandatory module "*Ethical Hacking and Penetration Testing*," bringing essential **technical depth** to the programme. This underpins its leadership in advising areas related to **cyber operations**, **incident response**, and **digital evidence management**.

Curated Pathways:

- Cyber Threat Intelligence Specialist
- Cybersecurity Auditor

Advising Themes:

- Security operations and threat detection
- Malware analysis, digital forensics, and chain of custody
- Infrastructure design, cloud security, and automation
- Cybersecurity technology and applications

This structured distribution of advising responsibilities ensures that students are matched with mentors who bring both **domain-specific expertise** and **institutional leadership** in their area of interest. At the same time, the cross-institutional nature of the programme encourages collaborative supervision and integrated support across all areas of the cybersecurity management spectrum.

Whom to Contact for Academic Advising?

- If you are enrolled in a **professional pathway**, please reach out to the **programme coordinator of the pathway's curating institution**.
- If you are **not enrolled in any pathway**, contact the coordinating institution (UDS) for academic supervision.

Your Contacts at a Glance:

Your Profile	Institution	Contact
Chief Information Security Officer (CISO)	UDS	coordinator.uds@digital4security.eu
Cybersecurity Educator	UDS	coordinator.uds@digital4security.eu
Cyber Legal, Policy, and Compliance Officer	MTU	coordinator.mtu@digital4security.eu
Cybersecurity Risk Manager	MTU	coordinator.mtu@digital4security.eu
Cyber Threat Intelligence Specialist	UNIR	coordinator.unir@digital4security.eu
Cybersecurity Auditor	UNIR	coordinator.unir@digital4security.eu
General Advising (no profile selected)	UDS	coordinator.uds@digital4security.eu

Library Services

As part of the Digital4Security platform, students have access to a digital library, including academic journals and resources relevant to the programme's core areas. Guidance is available as part of the Welcome Module training materials to help you evaluate sources, navigate scholarly databases, and reference works appropriately, whether human- or AI-generated.

Responsible: UDS
Contact: **coordinator.uds@digital4security.eu**

IT Helpdesk Service

Technical support is available for any digital learning issues you may encounter. Whether you are facing login troubles, access issues, or technical questions, the IT helpdesk is here to help.

Responsible: UDS
Contact: **IT@digital4security.eu**

Learning Development Support

Students may optionally choose to enable personal learning analytics to support their academic development. This feature uses course data to detect patterns that predict strong or weak performance, offering tailored, evidence-based feedback.

For example, active participation in teamwork and forum discussions may correlate with higher assessment scores for an individual learner, indicating the potential value of collaborative learning for them. By contrast, patterns such as frequent late-night work or last-minute submissions may be linked to lower grades for the individual, suggesting that the learner could benefit from improved time management.

By engaging with these patterns, students can learn to derive insights from their own learning data and apply practical strategies to refine their study habits. Supporting materials are provided as part of the Welcome Module training resources to help students build and strengthen effective learning habits. These skills will benefit participants not only throughout the programme, but also in lifelong learning beyond graduation.

Responsible: UDS
Contact: **coordinator.uds@digital4security.eu**

10.2 Personal Support

Equal Opportunities Service

The Digital4Security platform is designed with accessibility in mind, including features such as screen reader compatibility and simplified navigation to support students with visual, auditory, or mobility impairments (Section 14).

In addition to these built-in tools, we offer tailored support to ensure that students with special learning needs or disabilities receive the accommodations they need, including personalised guidance on selecting and using assistive technologies.

Furthermore, the service team provides guidance to instructors on designing inclusive learning materials, ensuring that each module is accessible and appropriate for a diverse student audience, including those with special needs. Respective recommendations are detailed in the *Practical Guide for Lecturers*.

Students are also encouraged to share personal tips and effective accommodations through a dedicated forum in the **Welcome Module**, helping peers customise their digital learning experience to suit individual needs and preferences.

Inclusivity is a community effort. If you are interested in launching a student-led initiative, such as a peer group or club focused on accessibility and support, we are happy to help facilitate outreach, tooling suggestions, and communication channels.

Responsible: UDS
Contact: **studyaffairs@digital4security.eu**

Student Counselling Service

Confidential support is available to help you manage personal challenges, academic pressure, or general well-being concerns. You are not alone. This service is here to help you stay resilient throughout your studies.

Depending on capacity, we currently offer one-on-one conversations. Should student numbers grow significantly, we may offer topic-centred group sessions in the future.

Curated resource collections developed by this service team are included in the **Welcome Module**, such as:

- Validated self-test scales to track levels of stress, depression, anxiety, bodily symptoms, and general wellbeing
- Guidance on interpreting your results on these scales, helping you recognise when professional support might be needed
- Pointers to freely available resources for stress reduction, self-help, mindfulness, and access to community or national health services

Please note: *While our programme offers supportive resources, they do not replace professional medical or psychotherapeutic care. If needed, we encourage you to prioritise services provided by licensed or government-approved health professionals.*

We also support student-led wellness initiatives such as online meditation, yoga, or fitness groups. If you would like to organise an activity, we are happy to assist with promotion, outreach, and selecting helpful digital tools to bring your idea to life.

Responsible: UDS
Contact: **studyaffairs@digital4security.eu**

10.3 Career and Skills

Industry Certification Services

To support your career development and signal your readiness for key cybersecurity roles, the programme integrates opportunities to earn **industry-recognised certifications** alongside your academic degree.

As part of your tuition, you are eligible to preparatory materials and special prices for **industry certification exams**. These certifications are aligned with the **European Cybersecurity Skills Framework (ECSF)** and can greatly enhance your visibility and credibility in the job market.

Each module is carefully reviewed for alignment with current industry standards. Where there is a strong fit, **certification recommendations** are included, helping you connect academic learning with professional credentials. For module-specific inquiries, you can contact the course instructor.

Where modules require **prerequisite knowledge**, or where students wish to upskill in a specific area such as technical competence, industry certifications may be recommended and can even be completed prior to enrolling in the Master's as preparation.

In addition, institutions curating the six professional pathways suggest **role-specific certifications** tailored to your chosen profile. For pathway-specific inquiries, you can contact the responsible programme coordinator.

Chief Information Security Officer – UDS
Contact: **coordinator.uds@digital4security.eu**

Cyber Legal, Policy, and Compliance Officer – MTU
Contact: **coordinator.mtu@digital4security.eu**

Cybersecurity Risk Manager – MTU
Contact: **coordinator.mtu@digital4security.eu**

Cyber Threat Intelligence Specialist – UNIR
Contact: **coordinator.unir@digital4security.eu**

Cybersecurity Educator – UDS
Contact: **coordinator.uds@digital4security.eu**

Cybersecurity Auditor – UNIR
Contact: **coordinator.unir@digital4security.eu**

The overall responsibility for the availability of industry certifications lies with the Coordinating Institution.

Responsible: UDS
Contact: **coordinator.uds@digital4security.eu**

Academic Writing and Research Support

Strong research and writing skills contribute to your success in this master's programme. They are also valuable assets for your future professional journey. To support you in developing these competencies, we offer streamlined support throughout your studies.

Your journey begins with the **Welcome** Module, which includes a concise introduction to evaluating source materials and citing them properly, whether the content is human-authored or AI-generated. This foundational guidance helps you start on solid footing and well-prepared.

In particular, your lecturers will indicate if and how AI tools may be used when preparing your assignments, and where such tool use is not permitted (cf. Section

6). Whenever AI usage is allowed, proper citation is expected, as taught in the **Welcome Module**.

Please note: *Unacknowledged AI usage may be treated as academic misconduct and, in severe cases, could result in disciplinary action (cf. Section 6.6). Understanding how to reference such sources correctly is therefore essential, and the relevant guidance is included in the Welcome Module.*

The **Welcome Module** also includes templates for slide presentations, written homework submissions, and the final thesis.

For more systematic skill development, academic writing and research support is embedded directly into the curriculum. All students complete a **Thesis** module with regular guidance from instructors and a dedicated supervisor to support the entire thesis-writing process. Additionally, the **Research Methods** module offers a comprehensive overview of research design and methodologies relevant to cybersecurity and digital governance.

Students interested in applied or collaborative research are also encouraged to explore opportunities within the UDS **Research Centers**, described below.

Support for the development of your academic writing and research skills is provided by instructors and mentors from the various institutions contributing to this master's programme. Overall responsibility for this area of student support lies with the coordinating institution.

Responsible: UDS
Contact: **coordinator.uds@digital4security.eu**

Student Mentoring and Support by Industry Experts

As a direct benefit from the Digital4Security project, students of this Master's Programme have the opportunity to receive **mentoring and support from senior**

industry experts. This unique service connects you with experienced professionals who can guide your learning, help you explore career paths, and provide insights from real-world cybersecurity practice.

Here is how the Digital4Security Grant Agreement defines the service, which is open to all students in this Master's degree programme. You have access to:

> Student mentoring & support by senior experts selected from [the] Industry Advisory board, industry partners from the consortium, participating SMEs and Companies, and other leading European and International firms. Students can select their industry mentors from a panel each year, or they can 'buddy' with the staff of participating companies to get involved in joint projects / cybersecurity challenges and gain more real-world experience. The Digital Learning Platform will provide a matchmaking tool to allow industry experts from the consortium and participating companies to post their interest in being involved, and for students to review the panel and request suitable experts. The consortium industry partners will ensure a comprehensive panel of cybersecurity management experts is available to support each student during each intake
> (Digital4Security Grant Agreement, p. 84f.)

Responsible academically: UDS
Contact: **coordinator.uds@digital4security.eu**

Facilitating body: Industry Advisory Board
Contact: **advisory-board@digital4security.eu**

Weekend Workshops, Networking Events and Guest Lectures

As another great benefit of the Digital4Security network, students have access to regular hot-topic events that bring together international European faculty, industry professionals, and organisations from across the entire partner network. These sessions combine practical case studies, expert presentations, hands-on workshops, and collaborative team activities, creating an engaging environment to explore emerging trends in cybersecurity and digital management.

The Digital4Security Grant Agreement describes the service as follows, which is open to all students in this Master's programme:

> Series of Weekend Workshops, Networking Events with Guest Lectures to bring together the students, faculty, experts and companies participating in D4S at regular events. The events will include digital skills experts and business leaders presenting real case studies from industry and talks on specialist cybersecurity management and technical subjects, along with other interactive workshops, projects and team activities [...]. The events will be designed to be hybrid, enabling large scale participation for all students even if they can't travel. The format of each event will be linked to a specific technology area or hot topic that will ensure maximum interest and engagement.
> (Digital4Security Grant Agreement, p. 85)

Responsible for academic events and programme integration: UDS & UNIR
Responsible for industry events: Industry Advisory Board
Contact: **advisory-board@digital4security.eu**

Career Weeks in Germany

Students enrolled in this programme are eligible to participate in *Career Weeks*: a short-term immersive experience designed to connect your online learning with real-world, on-site experiences. Organized by UDS in Germany, this four-week programme includes internships at regional companies in the Berlin–Brandenburg area, as well as professional skills workshops, cultural activities, networking events, and more. Support for travel logistics and housing is available. For details, see Section 17.3.

Responsible: UDS
Contact: **studyaffairs@digital4security.eu**

E-College Membership for Aspiring Entrepreneurs

As a student of this master's programme, you have **free access to the Entrepreneurship College (E-College)** at the Coordinating Institution, UDS.

The E-College is a hub for digital entrepreneurship, offering a rich blend of **education, mentoring, resources, and networking opportunities**. Whether you are looking to launch a startup, transform an idea into a viable business, or simply strengthen your entrepreneurial mindset, the E-College provides the tools and support to help you thrive.

You will benefit from access to:

- **Virtual incubator programs** with expert mentorship and peer collaboration
- **Hands-on workshops** in business model development, fundraising, and digital innovation
- A growing **network of entrepreneurs, alumni, and industry professionals**
- **Funding opportunities** and shared digital workspaces

You are invited to join this dynamic community that empowers future-oriented leaders and innovators to shape the digital economy.

More information: **Website Link**
Responsible: UDS
Contact: **coordinator.uds@digital4security.eu**

10.4 Community Life

Events and Networking

As a student in the Digital4Security Master's Programme, you are part of a vibrant European community of cybersecurity excellence. Across the Digital4Security network, you will find **numerous opportunities to connect, collaborate, grow professionally – and have fun.**

Partner institutions regularly offer:

- Guest lectures and expert webinars
- Hands-on workshops and cybersecurity challenges
- Hackathons and simulations
- Bootcamps, internships, and job placement initiatives
- Networking events across industry and academia

All activities can be attended **virtually**, but **on-site participation** may also be available for many events, offering the chance to connect in person and explore different parts of Europe.

You are also warmly invited to **attend and contribute** to the *Future of Learning Convention*: a flagship event of the programme, as detailed in the Internal Quality Handbook. This annual gathering brings together students, educators, researchers, and professionals to reimagine the future of digital education, particularly in the context of cybersecurity and the Digital4Security programme.

Beyond this, you may also participate in academic conferences hosted by UDS or other partners. Information about access and participation opportunities will be regularly communicated to enrolled students, helping you gain valuable experience and visibility in the field.

Have your own ideas for events or student-led services? The **Study Affairs** team is eager to support your initiatives, from clubs to community events. For example, you might consider organizing a party or music festival in the 3D Campus of Virtual Education (COVE) – see below. If you have a vision, we are here to help bring it to life.

Overall, many partners contribute to this rich extracurricular environment, and it is precisely this plurality that makes it such a valuable asset to students. Formally, the coordinating institution holds responsibility for providing a supportive structure and serving as a point of contact.

Responsible: UDS
Contact: **studyaffairs@digital4security.eu**

Mobility and Visa Support

As part of your student experience in the Digital4Security master's programme, you have access to various forms of mobility and visa-related support. Whether you plan to study fully online or participate in optional on-site activities – such as networking events, hackathons, or career weeks – guidance is available to help you make the most of your time as a student in an international programme.

Letters of invitation can be issued to support visa applications for official programme events, and some partner institutions also offer **local services** to assist with logistics. Students interested in short-term mobility may also receive help applying for **Erasmus+ opportunities**.

Please note: *visa fees, housing, and travel costs are* ***not*** *covered by your tuition and must be planned independently.* However, tailored support is available for some opportunities, such as participation in the **Career Weeks in Germany** (Section 17.3).

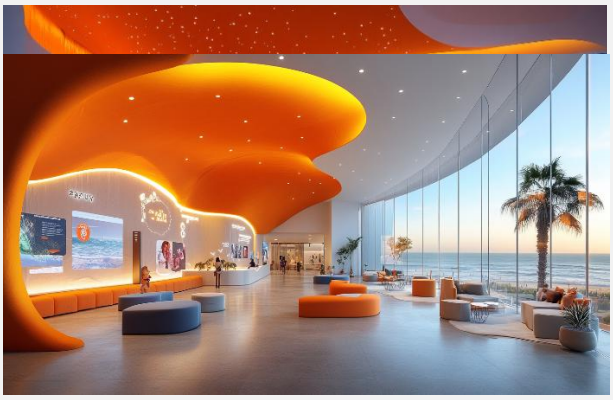
For further details on mobility, working alongside your studies, and guidance on what your tuition fee covers or does not cover, please consult **Section 17: Practical Info.**

Overall, mobility support (including letters of invitation for visa applications) is provided by various partners across the Digital4Security network whenever on-site attendance is offered for programme events. Final responsibility for these efforts lies with the coordinating institution.

Responsible: UDS
Contact: **studyaffairs@digital4security.eu**

Campus of Virtual Education (COVE): Your Immersive Learning Space

As a student in this master's programme, you are invited to use the **Campus of Virtual Education (COVE)**. More than a digital replica of a physical campus, COVE is a fun virtual space designed to inspire learning, creativity, and collaboration in the digital age.



COVE offers you the opportunity to participate in virtual lectures, explore 3D spaces like virtual labs, and collaborate with fellow students and faculty in uniquely designed settings, such as cliff-side lecture halls, sea-view libraries, and customisable digital dormitories.

As a student in this master's programme, **you are eligible to receive your own personal space on campus**, which can be customised with 3D assets and used for study, experimentation, or team collaboration.

As the campus continues to grow – with new buildings, activities, and student-led projects – so do your opportunities to explore, connect, and innovate within a truly 21st-century immersive virtual setting.

More information: **Website Link**
Responsible: UDS
Contact: **coordinator.uds@digital4security.eu**

10.5 Applied Research and Innovation

Application and Innovation Opportunities

The Digital4Security network provides a rich environment for engaging with real-world cybersecurity challenges.

As a student, you can take advantage of:

- **Internship opportunities** and **industry mentoring** offered by partners across the Digital4Security network, as communicated via the learning platform.
- **Project-based thesis opportunities**, allowing you to embed your research in practical contexts such as SMEs, policy bodies, or research labs. This may include thesis proposals addressing current challenges in cybersecurity, data governance, or digital transformation.
- **Access to applied research and training labs offered by Digital4Security partners**, providing spaces for experimentation, design, collaboration, and learning. For instance, **Cyber Ranges** offer immersive, high-fidelity environments where you can develop and test cybersecurity skills. Their virtual

platforms simulate real-world networks and advanced cyber threats, enabling safe, hands-on learning in dynamic and realistic scenarios.

These opportunities are made possible through the strength and diversity of the Digital4Security partnership network. The coordinating institution holds responsibility as the official point of contact for inquiries or suggestions.

Responsible: UDS
Contact: **coordinator.uds@digital4security.eu**

Membership in a Research Centre

If you are looking to deepen your academic journey – especially toward the end of your studies or when considering a PhD – you are warmly invited to engage with the **Research Centres** at UDS.

These centres serve as dynamic, interdisciplinary hubs where professors, researchers, postgraduates, and doctoral candidates collaborate on innovative research at the forefront of the digital era. Each Research Centre offers expert supervision, research paths, and the chance to contribute to impactful projects.

As a student in this master's programme, you have the opportunity to:

- Become a member of one or more Research Centres
- Join cutting-edge research projects aligned with your interests
- Co-author academic publications and conference papers
- Receive mentorship from experienced researchers and professors
- Engage in workshops, seminars, and colloquia hosted by Research Centres
- Explore pathways into doctoral studies

Current focus areas of the Research Centres include:

- **Cybersecurity**: Human factors, economics of security, and AI-driven threat analytics

- **Artificial Intelligence**: Machine learning, big data, and deep learning applications
- **Educational Technologies**: Learning analytics, generative AI, and digital pedagogy
- **Extended Reality**: Research in VR/AR environments for education, health, and industry
- **Digital Transformation**: Policy, science, and society in the digital age

The Research Centres provide a welcoming and intellectually stimulating environment where your curiosity, skills, and ambitions can thrive. Whether you are preparing a thesis, exploring a research career, or seeking to make a scholarly contribution, these centres offer support and structure to take your ideas further.
More information: **Website Link**
Responsible: UDS
Contact: **coordinator.uds@digital4security.eu**

D-College Membership for Aspiring Innovators

As a student in this Master's programme you have **free access to the Design Thinking College (D-College)** at the Coordinating Institution, UDS.

The D-College is a centre for innovation and collaborative problem-solving. Rooted in the principles of Design Thinking, it offers a unique space to explore how creative and analytical thinking can drive digital transformation. Whether you are tackling a research challenge, designing a new service, or leading organizational change, the D-College equips you with the mindset and tools to innovate effectively in a complex world.

Through the D-College, you can engage with:

- Workshops, training formats, and research opportunities focused on design-driven innovation
- Interdisciplinary collaboration with students, researchers, and external partners

- For students towards the end of their studies and transitioning to a phd: Access to the D-Colloquium, a biweekly hands-on space for joint project work
- For all students: A flexible hybrid learning environment, from real-world retreats to extended reality sessions with dedicated events, trainings and resources
- A dynamic online Design Thinking community promoting openness, creativity, and shared growth

The D-College empowers students to apply design thinking to societal, organizational, and technological challenges, making it a supportive environment for innovators to shape the future of cybersecurity, digital governance, and beyond.

More information: **Website Link**
Responsible: UDS
Contact: **coordinator.uds@digital4security.eu**

11. Quality Assurance: Shaping a World-Class Programme Together

Quality assurance in this Joint Master's Programme is more than a regulatory obligation. It is an opportunity for collaboration and building a shared culture. We want to empower students, instructors, staff, and industry experts to contribute to shaping how the programme grows and improves.

This section provides a brief overview of quality assurance, including how you can share your observations, contribute suggestions, and actively co-design the future of the programme. Full details are available in the **Internal Quality Handbook**, and an introductory video is provided in the **Welcome Module**. Guidance on where to find this programme resources is provided by the end of this document.

11.1 What Can and What Cannot be Changed

All adaptations in this programme occur within the boundaries set by the **European Approach for Quality Assurance of Joint Programmes** and the relevant national regulations. Certain core elements are fixed and cannot be modified without a formal re-accreditation process. These include the list of modules, the overall programme structure, the learning outcomes at both programme and module level, the total number of ECTS credits, and the awarding institutions.

At the same time, many other aspects remain flexible and responsive to new developments. These include the learning resources provided, the approaches used in student services, extra-curricular offerings, and community-building initiatives such as clubs, mobility opportunities, and other support structures. Options for industry certifications may also evolve over time.

Within individual modules and the broader e-learning strategy, numerous elements can be refined. These include the design of learning activities and assessments (while maintaining the required 60% proctored examination component),

as well as the integration of newly relevant topics in response to ongoing developments in cybersecurity. Collaborative tools, such as forums, may also be adapted or expanded to better support academic dialogue, community engagement, and project-based collaboration.

The programme's quality assurance mechanisms are likewise subject to continuous enhancement, including the methods used for data collection and analysis. A key area where student input is especially valued is in assessing the compatibility of study requirements with work and family responsibilities. Your observations help in understanding what works well or what could be improved to better support balance and well-being.

Many students also bring valuable professional experience into the programme. Suggestions for aligning assessments with real-world challenges are particularly welcome, as they can help ensure academic tasks generate immediate value for both your learning and your workplace.

In addition, student perspectives can inform our outreach and inclusion efforts, helping us further diversify and strengthen the learning community. Bottom-up initiatives related to student life or project collaboration beyond the formal curriculum are also highly welcome.

Employability is another key focus. Networking, mentoring, project and thesis work, case studies, tools, and assessments can be refined based on input from students, alumni, the Industry Advisory Board, and other stakeholders to align with real-world practice and support career development.

Overall, this programme is designed not only to equip you with advanced knowledge, skills, and competencies as an individual. It also aims to foster a vibrant, connected culture and professional network: one that supports you during your studies, while it also continues to create value long after graduation, as we work together to build a more secure digital future.

11.2 Programme Goals

The 60 ECTS Online Master's Degree in **Cybersecurity Management and Data Sovereignty** is designed to support the following seven core goals. These goals also reflect the long-term vision of the **Digital4Security** project, extending beyond the period of EU co-funding.

The programme's internal quality assurance mechanisms play a central role in ensuring these goals are met and continuously improved upon. This involves close listening and insightful reflection based on feedback from students, alumni, lecturers, and industry experts, as well as data-driven analyses. The programme is committed to innovation and designed to remain agile in adapting its approaches to maximise the achievement of these objectives.

1. Cybersecurity Leadership
Foster the advanced knowledge, skills, and competencies needed to lead cybersecurity initiatives, enabling graduates to make well-reasoned decisions, drive proactive risk management, and shape organisational cybersecurity practices effectively.

2. Excellence in Online Education
Deliver a high-quality, fully online learning experience that combines applied project work, stakeholder engagement, and personalised learning pathways, equipping learners to achieve their career goals and apply knowledge in real-world contexts.

3. Lifelong Learning
Support ongoing professional development through flexible, modular study options that enable reskilling, upskilling, and agile adaptation to emerging threats, technologies, and regulatory environments.

4. Industry-Aligned Education
Ensure the curriculum and assessment address current and emerging industry needs, preparing learners for management and leadership roles across enterprises, SMEs, and the public sector.

5. European Sovereignty
Develop expertise in cybersecurity management and data governance that advances the EU's strategic autonomy and safeguards digital infrastructures across critical sectors.

6. Inclusion, Accessibility and Gender Equality
Promote accessibility, gender balance, and inclusion of underrepresented groups by removing participation barriers and fostering a diverse cybersecurity talent pipeline.

7. Responsible Innovation and Ethics in Cybersecurity
Foster ethical reasoning, legal understanding, and social awareness to promote responsible, foresighted leadership and regulatory compliance.

11.3 Internal and External Quality Assurance

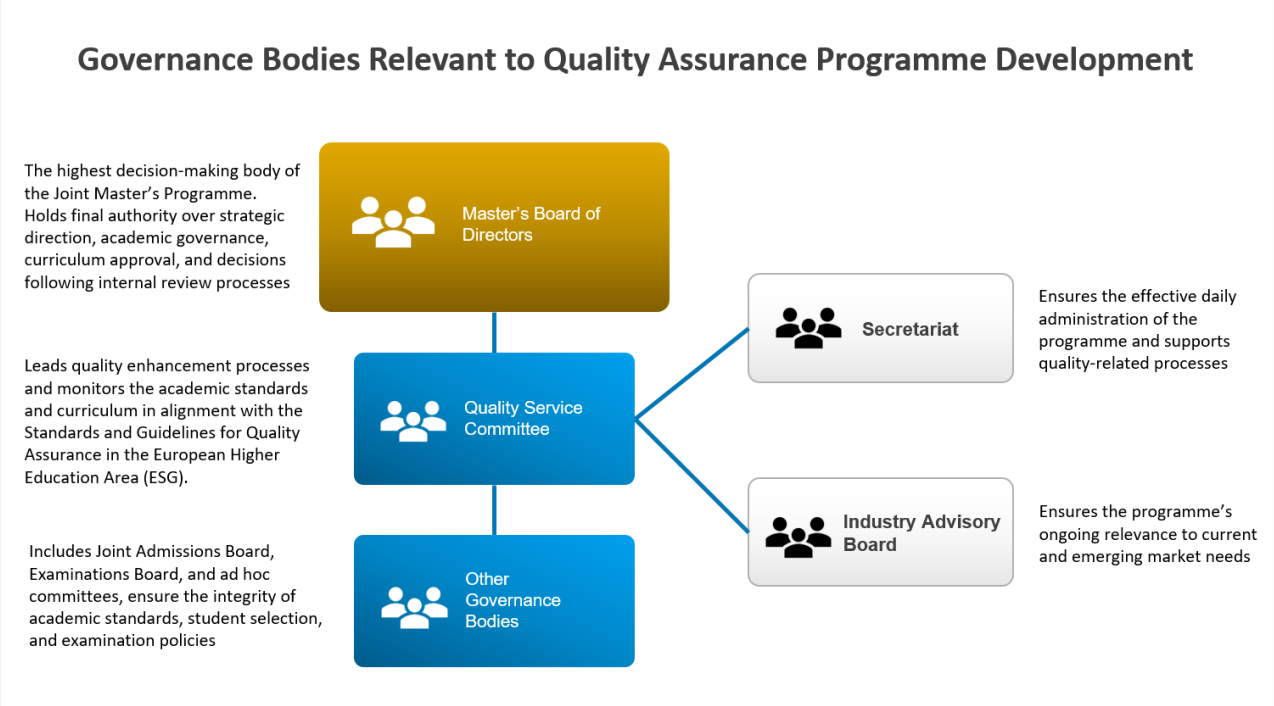
The programme is guided by rigorous quality assurance processes that follow the **Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG)**. These include both internal mechanisms – such as student surveys, module reviews, and course analytics – as well as external oversight through **European and national accreditation reviews,** complemented by r**egular assessments via the Industry Advisory Board (IAB)**. This dual approach helps to ensure academic excellence, regulatory compliance across different systems, and real-world relevance for cybersecurity professionals.

The **Master's Board of Directors** holds final authority over the programme's governance. It is supported by the **Quality Service Committee**, a dedicated body focused on enhancing your learning experience, refining teaching approaches, and ensuring the curriculum stays aligned with evolving industry needs.

Importantly, **student representatives are full, voting members** of the Quality Service Committee. They actively contribute to voicing student experiences and priorities – ensuring your perspectives are not only heard, but help to shape the future of the programme.

Figure 9 provides an overview of the key bodies involved in the ongoing quality assurance of the programme.

Figure 9: Quality assurance structure of the Joint Master's Programme.



At the heart of continuous quality review is the Quality Service Committee. Supported by the Secretariat and drawing on insights from the Industry Advisory Board, student surveys, and other feedback mechanisms, this committee analyses data and proposes improvements to the programme. Final decisions on these proposals are made by the Master's Board. Subsequently, decisions are implemented by all bodies and partners.

11.4 Accreditation

This Joint Master's Programme is developed under the **European Approach for Quality Assurance of Joint Programmes**, ensuring it meets rigorous academic standards recognised across the European Higher Education Area (EHEA). The programme is currently undergoing accreditation by **ASIIN**, a recognised quality assurance agency officially listed in the European Quality Assurance Register for Higher Education (EQAR) [statement subject to ongoing developments].

The European Approach was introduced in 2015 by the Ministers of Higher Education across the EHEA to streamline quality assurance for joint degrees offered by universities in multiple countries. One important goal is to enable truly European

study experiences for students by removing administrative barriers where possible and awarding internationally recognised degrees aligned with shared European standards (ESG). The **ESG** – **Standards and Guidelines for Quality Assurance in the European Higher Education Area** – define how academic quality, student-centred learning, and institutional accountability are ensured across Europe.

Overall, you are enrolling in a programme that is "Europe-powered" in many regards. As the official EQAR site explains:

> Joint programmes are a hallmark of the European Higher Education Area (EHEA). They are set up to enhance the mobility of students and staff, to facilitate mutual learning and cooperation opportunities and to create programmes of excellence. They offer a genuine European learning experience to students.
> (EQAR, 2025)

You can visit the website to learn more: https://www.eqar.eu/kb/joint-programmes/

In addition, each awarding university – UDS (Germany), MTU (Ireland), and UNIR (Spain) – ensures national recognition through country-specific accreditation procedures.

This means your degree is fully recognised in Germany, Ireland, and Spain, and valid throughout the EHEA and beyond, supporting both academic progression and international employability.

11.5 Your Experiences Matter – Please Share them

Your experiences and suggestions play a vital role in shaping the programme. Throughout your studies, you will be encouraged to share insights and ideas through various channels, including:

- Module evaluations
- Programme-wide surveys (e.g., on platform usability and e-learning experience)

- Student representation in committees and working groups
- Open feedback channels on the learning platform
- The Future of Learning Convention, an annual event where students, faculty, and industry partners come together to share experiences and co-create programme improvements

All feedback is treated seriously, typically anonymized unless you indicate otherwise, and carefully analysed to emphasize insights and patterns. Where appropriate, improvements are implemented promptly and responsibly.

11.6 Continuous Monitoring and Improvement

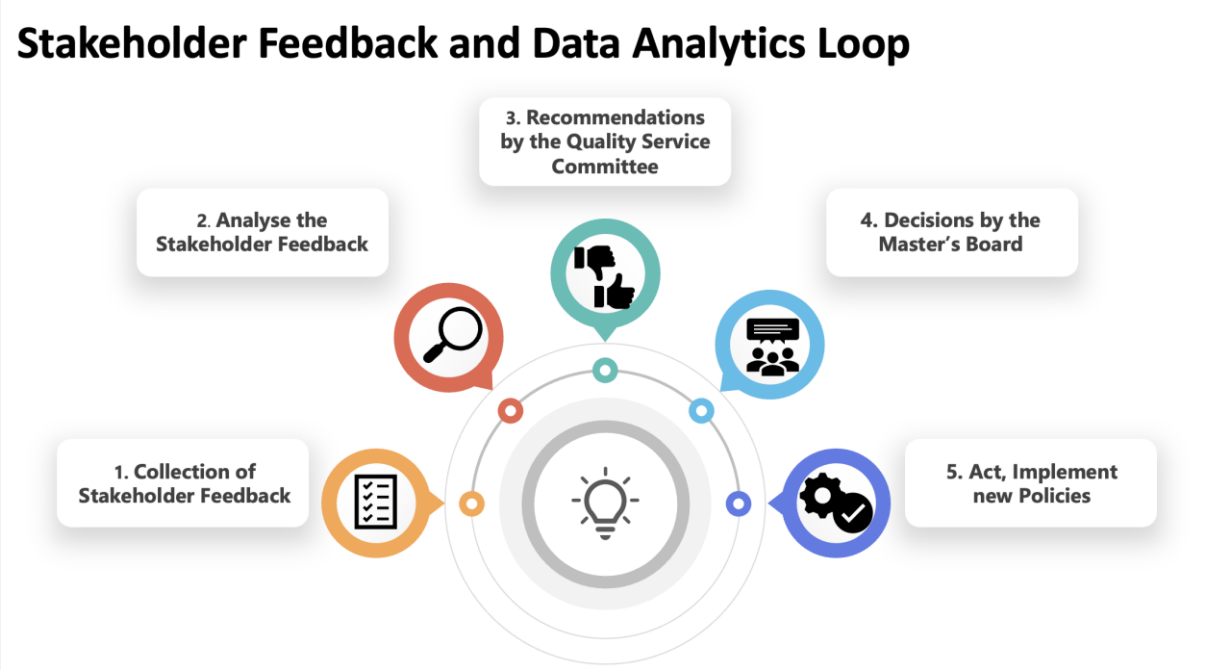
We use a range of quality data sources to keep improving, such as:

- Student survey feedback
- Anonymised platform data
- Course progression records
- Lecturer self-reflections
- Academic peer reviews and industry partner reviews of course content and assessments
- Alumni and employer feedback

Insights and trends are summarised in the **Annual Programme Review Report**, which guides strategic enhancement and programme updates.

The overall procedure for quality assurance is illustrated in Figure 10.

Figure 10: Quality assurance cycle of the Joint Master's Programme.



Through multiple feedback and data-gathering channels, the Quality Service Committee formulates evidence-based suggestions for programme improvement. These are reviewed and decided upon by the Master's Board. Once approved, changes are implemented collaboratively by the relevant programme bodies to ensure continuous enhancement of the learning experience.

11.7 Mastering Feedback: I Like, I wish, and Clarify

If you have ideas or concerns, please share them. If something inspires you, celebrate it with us. Quality in education is not a fixed goal or threshold. It is a shared process and culture. Together, we make this programme stronger, more inclusive, and future-ready.

One simple and effective method we encourage is the **"I Like, I Wish, and Clarify"** approach. While formally embedded in the quality assurance framework outlined in the **Internal Quality Handbook**, it is also a valuable soft skill and cultural practice across all our interactions.

You are invited to use this approach when giving feedback: both within individual modules and on the programme as a whole.

- **I like** – Highlight what worked well for you or helped you succeed. This allows us to preserve what matters most, and to learn from strong examples that could inspire other modules or approaches.
- **I wish** – If you encountered a challenge or felt something was missing, let us know. Ideally, go beyond what didn't work or frustrated you, and share what you think might help instead. Suggestions are especially welcome.
- **Clarify** – If you feel confused, stuck, or uncertain, don't hesitate to ask. Let us know what kind of information, format, or guidance would help you feel more oriented and confident in taking action.

Thank you for being an active part of this evolving learning community, and for co-shaping a programme that becomes more relevant, inclusive, and rewarding with each new contribution.

12. Legal Framework of the Programme

The 60 ECTS Online Master's Programme in Cybersecurity Management and Data Sovereignty is governed by a robust legal foundation that ensures academic quality, student rights, and cross-border recognition of your degree. As a joint programme delivered across Germany, Ireland, and Spain, it complies with national legal systems as well as shared European standards for joint degrees and quality assurance.

12.1 National Legal Foundations

Each awarding institution operates within national, regional, and institutional legal frameworks, all of which are reflected in the overall programme regulations. These frameworks ensure full compliance with both local legislation and overarching European standards. Key regulatory references include:

- **Germany**: The programme is aligned with the *Brandenburgisches Hochschulgesetz* (Brandenburg Higher Education Act), with particular relevance to sections on joint degree programmes, examination law, and student rights.
- **Ireland**: The programme follows the *Qualifications and Quality Assurance (Education and Training) Act 2012*, which governs programme validation, quality assurance, and the awarding of qualifications.
- **Spain**: Compliance is ensured with *Real Decreto 822/2021 and Ley Orgánica 2/2023*, which regulate the organisation of university education in Spain, alongside relevant regional laws.

In addition, the programme meets the requirements of the *European Approach for Quality Assurance of Joint Programmes*.

12.2 Cooperative Governance

The core legal and administrative principles of the programme are outlined in the Joint Programme **Cooperation Agreement**, which defines how the awarding institutions collaborate, how academic and administrative responsibilities are shared, and how decisions are made.

Key governing documents furthermore include:

- The **Study and Examination Regulations**, which detail assessment procedures, grading, and student obligations;
- The **Internal Quality Handbook**, which explains the quality assurance mechanisms;
- The **Student Handbook** you are currently reading, which aims to provide accessible guidance on rights, responsibilities, and practical matters during your studies.

12.3 Data Protection

The master's programme is fully compliant with the **General Data Protection Regulation** (GDPR), applicable across the European Union. All partner institutions follow national implementations of GDPR and ensure that your personal data is handled securely, transparently, and only for educational and administrative purposes.

The body responsible for facilitating the programme's data protection, providing relevant staff training and guidance is the **Joint Admissions Board**, which can be contacted via **online.admissions@digital4security.eu**.

Each degree-awarding institution also appoints a designated representative responsible for ensuring student data protection and GDPR compliance, as coordinated by the Joint Admissions Board: the institutions' Data Protection Officers (DPOs).

12.3.1 Guidance for Participation in Synchronous Study Sessions

Modules in this programme include live online sessions, which are routinely recorded so that students unable to attend in real time can still benefit from access to the material. These recordings are accessible only to students enrolled in the relevant module and the programme's teaching staff.

To protect your privacy and that of others, please take care when contributing to live sessions. Do not share any personal or sensitive information that you would not wish to appear in a recording. This includes details such as health conditions, financial matters, or confidential information from your workplace.

When you participate in discussions, you are responsible for ensuring that the information you provide is appropriate for a learning environment where recordings are made. If you wish to raise a matter that is sensitive or private, we encourage you to contact your lecturer or programme coordinator directly outside of the recorded session.

By being mindful of what you share, you help create a safe, professional, and respectful learning space for yourself and your peers.

12.3.2 Your Data Protection Rights as a Student

Under the General Data Protection Regulation (GDPR), you have several rights concerning the personal data held about you by the programme. These rights are designed to give you control over your personal data and ensure that it is accurate, secure, and processed responsibly.

At the same time, it is important to note that certain information must lawfully remain part of your official student record and cannot be erased or altered, since it is required to demonstrate your academic achievement, to issue your qualification, or to comply with legal, contractual, or accreditation obligations.

Retention periods in this programme:

- **Degree-relevant documentation** is securely maintained for 50 years after you graduate or withdraw from the programme, in line with the most stringent European regulations (for example, modules completed, grades, degree certificate, and diploma supplement). This ensures that you can access proof of your achievements and qualifications well into the future.
- **Live session recordings** within modules are retained for a maximum of 1 year and then permanently deleted, in accordance with data protection requirements.

Your rights under GDPR include:

- **Right of access** – You can request a copy of the personal data held about you, such as your official student record (modules completed, grades, progression) or personal details (e.g., contact information).
- **Right to rectification** – You can ask for corrections if your data is inaccurate or incomplete. For example, if your name is misspelt, your contact details are out of date, or there is an error in your recorded grades, you may request and support rectification.
- **Right to erasure ("right to be forgotten")** – You may request that certain personal data is deleted. For example, if in a demographic survey you chose to share personal life circumstances that you later decide you would prefer to keep private, you may request that your response be removed from the data set. However, records necessary to maintain the integrity of your qualification (e.g. your module grades, final award, or involvement in formal procedures) must be retained as long as legally required.
- **Right to restriction of processing** – You may request that the use of your data be limited in particular circumstances. For example, if you temporarily withdraw from the programme for personal reasons, you may request that your data is not actively used for communications until you return.

- **Right to object** – You may object to certain forms of data processing. For example, you can choose whether to activate or deactivate learning analytics that give you feedback on how your study patterns relate to your subsequent module grades or self-reported course satisfaction.
- **Right to data portability** – You may request personal data in a digital format, enabling you to re-use or share it. For example, you may download your transcript of records to present for an application elsewhere.

How to exercise your rights:

Self-service records – Through the programme's fully online system, you can generate and download many documents yourself. The Welcome Module offers a brief introduction. This means you can quickly access key records without needing to make a formal request – a significant benefit of the digital infrastructure used in this master's programme.

Further requests:

- For **institution-specific matters**, please contact the Data Protection Officer (DPO) of UDS, MTU, or UNIR.
- For **general matters concerning your student record** (e.g., personal data and contact details, progression, grades, and final award), please contact the Secretariat.

For additional details on *Data Processing and Protection* in this programme, please consult your **Student Agreement**.

12.4 Document Hierarchy

In case of any inconsistencies or conflicting interpretations between programme documents, the following order of precedence applies:

1. Cooperation Agreement
2. Study and Examination Regulations
3. Internal Quality Handbook
4. Module Handbook
5. Student Handbook
6. Student Agreement
7. Other supporting documents

This order ensures that legally binding agreements and formally approved regulations take precedence over explanatory or sample materials.

Should you become aware of or suspect any inconsistencies between the programme documents, your message to **quality.committee@digital4security.eu** is much appreciated. It allows us to review the material and helps to ensure overall coherence.

13. Appeals

An appeal is a formal request to review or reconsider a decision that you believe was made unfairly or in error, ensuring that your rights as a student are respected and upheld.

We are committed to fostering a learning environment that is transparent, respectful, and fair. If you ever feel that an assessment outcome does not reflect your efforts or that a process has not been applied correctly, you have the right to raise your concerns. Appeals are a normal part of academic life and help uphold quality and integrity for everyone.

Further information is also available in the **Study and Examination Regulations**. Additionally, a video covering this subject is available in the **Welcome Module**. Guidance on where to find this programme resources is provided by the end of this document.

13.1 What You Can Appeal

You may appeal:

- A negative admission decision
- A grade you received for an assignment, project, or exam
- Peer review feedback you believe was unfair
- A suspected case of academic misconduct you have been involved in
- Behaviour of others that you perceive as disrespectful or unjust

Appeals are not only your right. They are also welcomed as a way to ensure decisions are well-informed and just.

13.2 Appeals on a Negative Admission Decision

If you applied to this Joint Master's Programme and received a **rejection you believe was unjustified**, you have the right to request a review of the decision.

- Submit a **written appeal** within **14 calendar days** of receiving the official admission result. This appeal shall be addressed to **online.admissions@digital4security.eu**, copying **secretariat@digital4security.eu** in Cc.
- Your appeal should clearly outline why you believe the decision was incorrect, and may include additional supporting information (e.g., documents not considered or misunderstood).
- The appeal will be reviewed by the **Admissions Committee**.
- A final, reasoned response will be sent to you as soon as possible, typically within 4 weeks.

Appeals are considered carefully and respectfully.

Please note that the admission criteria are firmly established through the Cooperation Agreement between the awarding institutions and have been reviewed and approved as part of the accreditation process. While you are entitled to appeal if you believe your application was not properly assessed based on these criteria, suggesting alternative admission requirements is not a valid basis for reconsideration.

13.3 General Grade Appeals

If you believe that a grade does not accurately reflect your performance, the first step is to **seek clarification through an informal assessment review session**. You can submit a request for this review to the responsible examiner within **one week** of the grade being issued. The examiner will then organise a review session, which should take place within one week of your request. It provides a valuable opportunity to discuss the evaluation in detail, gain insight into how the grade was determined, and raise any questions or concerns you may have.

In some cases, the examiner may choose to hold a joint review session for all students in the module rather than individual meetings. While individual appointments are not guaranteed, they may be offered at the examiner's discretion.

If, **after this informal review**, you still have concerns about your grade, you may submit a formal grade appeal. This appeal must be made in writing and **submitted within three weeks of the original grade's publication**. Your appeal should clearly explain the reasons for contesting the grade, referring to any relevant assessment criteria or grading rubrics provided. The formal appeal will initially be reviewed by the institution(s) responsible for the module. The case may be escalated from a Delivering Partner institution to the Module Guarantor Instutition in this phase.

Should the issue remain unresolved at this stage, the appeal may be escalated to the Examinations Board, and, if necessary, to the Master's Board of Directors, which acts as the final authority on grade appeals.

13.4 Appealing Peer Feedback

We value the power of peer learning and want to ensure that peer assessment is both meaningful and fair.

Peer review is used to deepen learning, build evaluative skills, and foster mutual inspiration in larger learning groups. In many cases, your work will be reviewed by several peers who completed the same exercise, and their scores will be averaged to form your result. You will also evaluate the work of others using shared criteria, developing your ability to give constructive feedback, reflect critically, and learn from diverse examples — all key skills for academic and professional growth.

If you believe that a peer assessment was **unfair**, the following steps apply:

- **Submit a written appeal** to the course instructor within **one week** of the peer grading publication. This can be done, for example, via Moodle's feedback or messaging system. Be sure to include a clear explanation of your concern.

- The instructor will **review your submission** and the relevant peer evaluations within **one week** of receiving your appeal.
- If your concern is **substantiated**, the grade will be **adjusted manually**.

If you remain dissatisfied with the outcome:

- The instructor-confirmed grade will count as the **official date of grade issuance**.
- You may then **request an informal grade review session** with the instructor **within one week** of that date, following the general grading complaints procedure described in Section 13.3 of this Handbook.

13.5 Academic Misconduct

If you are ever involved in a case of suspected academic misconduct – such as plagiarism, unauthorised collaboration, or cheating in an exam – rest assured that the process is designed to be **transparent, respectful, and supportive**. It aims to protect both academic integrity and your rights as a student.

What Happens if There's a Concern?

- **You will be informed** of the concern and given an opportunity to respond within **two weeks** of the formal notification.
- An **initial review** will be conducted by the **Examinations Board**.
- If needed, the matter may be escalated to the **Master's Board of Directors**.
- In more complex cases, a **Disciplinary Committee** may be convened. This Committee includes faculty from **at least two awarding institutions**.

What Sanctions Are Possible?

If a violation is confirmed, sanctions will be **proportionate** and, wherever possible, **developmental**. These may include:

- Constructive feedback or the opportunity to revise and resubmit the work
- Grade adjustment or nullification

- Temporary suspension from the programme
- Expulsion, in the most serious or repeated cases

How To Appeal?

You may **appeal any disciplinary decision in writing within 14 calendar days** of formal notification.

Your appeal should clearly explain the grounds for the appeal and must be submitted by email to **secretariat@digital4security.eu**, and also to the body that issued the original decision (the Examinations Board, a Disciplinary Committee, or the Master's Board).

You will receive a formal response as early as possible, and no later than **four weeks during active teaching periods** (excluding official breaks).

13.6 Addressing Unfair or Disrespectful Behaviour of Others

All students have the right to a safe, respectful, and inclusive learning environment. If you experience or witness behaviour by an instructor, peer, or staff member that feels **unfair, inappropriate, or disrespectful**, you are encouraged to speak up.

You may:

- **Contact the respective person**, offering constructive feedback (see Section 11.7 for inspiration)
- **Contact the Guarantor Institution** responsible for the module (see Section 4.2)
- **Contact your Programme Coordinator** (if signed up for a professional profile) or **studyaffairs@digital4security.eu** to seek advice or formally lodge a concern
- **Use the anonymous feedback channels** on the LMS to report an issue
- **Contact a student representative** who can raise the issue on your behalf
- **Contact the ombudsperson** for guidance (see Section 13.7)

Depending on the situation, concerns may be addressed informally through mediation, or formally via institutional procedures. Either way, your well-being and dignity are taken seriously, and support is available via multiple appointed individuals and organisational bodies. You can choose the communication pathway that best resonates with your situation and preferences.

13.7 Ombudsperson

An **ombudsperson** is a **neutral, independent contact person** who supports students when they encounter conflicts, feel they have been treated unfairly, or are unsure how to proceed with complaints or concerns, especially if other mechanisms have not resolved the issue. They:

- Act **independently of teaching and grading**
- Offer **confidential support and guidance**
- Help mediate **sensitive situations**, including conflicts with staff or peers
- Guide students through **appeals or complaint procedures**
- Recommend institutional improvements based on recurring patterns

In this master's programme, one or more ombudspersons are nominated by the Master's Board.

You can contact the ombudsperson(s) if:

- You feel a conflict with a peer or staff member has not been fairly addressed
- You need guidance on how to navigate formal complaint or appeal processes
- You experience unfair treatment or misconduct
- You seek confidential advice before raising a sensitive issue

The ombudsperson operates independently of academic grading and teaching and will listen without judgement. They do not take sides, but help find fair and respectful solutions, or guide you to the right process.

For this support, you can reach out to
ombudsperson@digital4security.eu

14. Introduction to the Digital Learning Environment

This master's programme is **delivered entirely online** through a digital learning environment. It consists of three main components, each serving a specific function throughout your student journey. Understanding how they work together will help you navigate the programme confidently, from your first inquiry to your regular studies.

14.1 Where Everything Begins: The Website

The starting point for every student is the official project website: **www.digital4security.eu**. Here, you can explore the programme in detail, review entry requirements, read about the consortium partners, and check the latest updates. If you are considering applying, the site provides clear information on tuition fees, the programme structure, and who the programme is designed for. When you are ready, you can click the “Apply Now” button to move to the next stage.

The **Digital4Security initiative** offers a comprehensive portfolio of educational opportunities designed to meet a variety of professional and academic needs. These include **microcredentials**, a **60 ECTS fully online Master’s programme**, and a **120 ECTS hybrid Master’s programme** that combines online and in-person learning. All programme options are described in detail on the Digital4Security website. You are encouraged to explore the information available there to determine which educational model best aligns with your situation and goals. When you have identified the right option, you can proceed directly to the application process via that website.

14.2 Managing Your Application and Profile: Full Fabric

Once you decide to apply, you will be directed to **my.digital4security.eu** – a portal powered by **Full Fabric**. This is your central hub for admissions and hosts your personal student profile.

Full Fabric supports all administrative aspects of your journey: from the initial eligibility check, through the submission of academic transcripts and your CV during the application process, to course registration and, ultimately, the issuing of your certificates.

At the start, you may spend a good portion of your time on this platform to complete the application and onboarding steps. After submitting your application documents, you can track the review progress in real time and may respond to any potential requests from the admissions team. Once you have been accepted, you will be invited to sign your Student Agreement, arrange your tuition payment, and select your courses for the first term.

When your enrolment is confirmed, your account will be automatically linked to the learning platform. This means you will not need to manage multiple logins, as access to all systems is unified.

Beyond admissions and enrolment, Full Fabric also serves as the long-term home for your academic records. Your module completion data, industry certifications (when conducted within the programme), the final degree certificate and your Diploma Supplement will be issued and stored here.

The programme guarantees that your certificates will be stored securely for at least 50 years. Should Full Fabric ever cease to operate, or should at some point the programme transition to another platform, you will be informed about where and how to access your documents moving forward. In case of any questions regarding the long-term storage of your credentials, you can contact the programme secretariat at

secretariat@digital4security.eu.

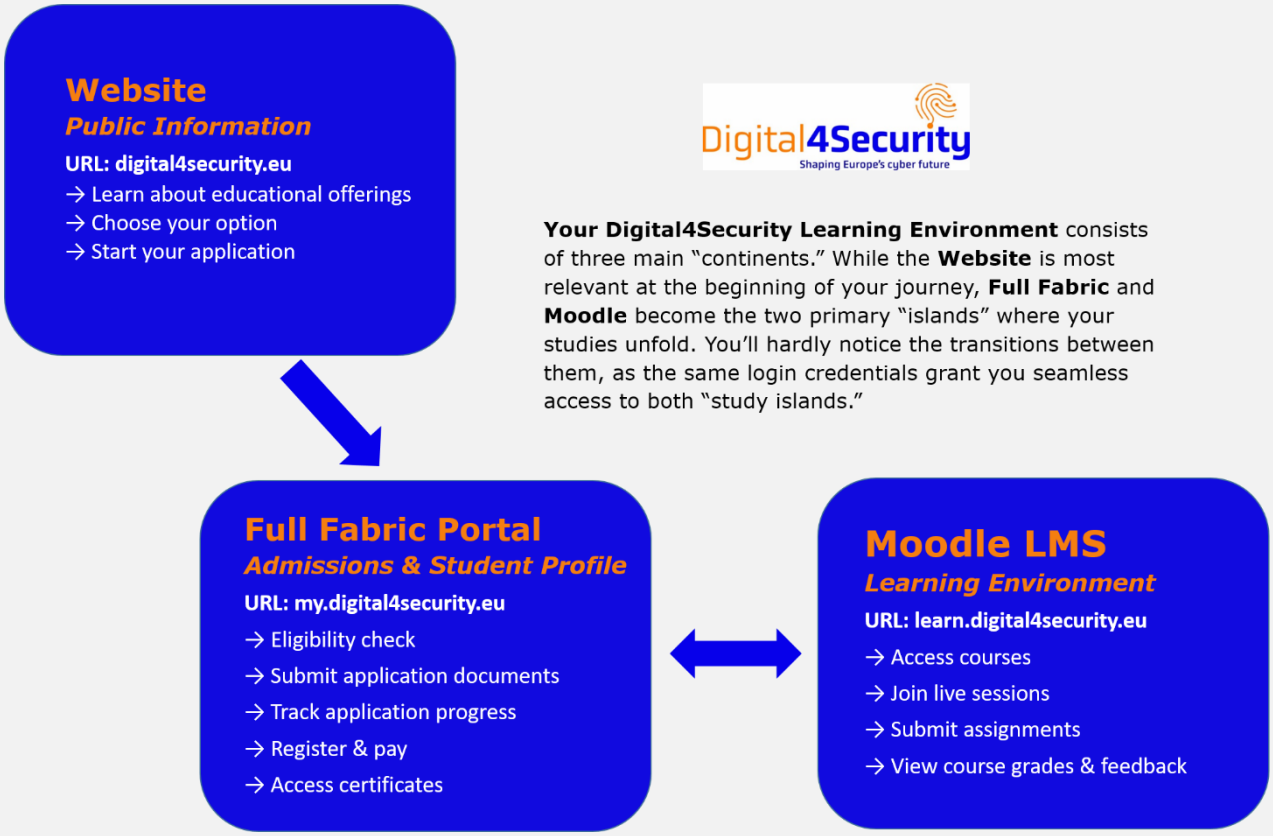
14.3 Your Virtual Campus: Moodle

Once enrolled, your learning will take place on **learn.digital4security.eu**, a dedicated Moodle-based Learning Management System. This is where you will access course content, participate in live sessions, complete assignments, interact with instructors and peers, and track your academic progress within courses. Moodle has been extensively customised to support both real-time and on-demand learning, with features such as the integrated BigBlueButton tool for virtual classrooms, interactive modules, and discussion forums.

Thanks to Single Sign-On (SSO) functionality, your login experience will be seamless: Upon enrolment, you will receive an automated email with credentials and instructions. From that point forward, you can move between Full Fabric and Moodle effortlessly, with the same login credentials.

An overview of your entire learning environment is provided in Figure 11.

Figure 11: A map of your learning environment, comprising three "continents:" the Website, Full Fabric and Moodle.



14.4 Support, Accessibility, and Data Protection on the Platform

The Digital4Security platform has been designed with responsiveness and accessibility in mind. Whether accessed via desktop, tablet, or mobile device, the interface remains intuitive and user-friendly. Key accessibility features – such as screen reader compatibility and simplified navigation – support students with visual, auditory, or mobility impairments.

Furthermore, technical support is available at multiple levels. Full Fabric provides assistance related to the application and enrolment process, while Moodle-related support is offered by Matrix Internet, who developed and maintain the platform.

Additionally, as the coordinating institution, UDS is responsible to help ensure the overall availability and functionality of the programme infrastructure. For specific concerns, please reach out to:

- **it@digital4security.eu** – for platform issues, login problems, or system access.
- **studyaffairs@digital4security.eu** – for support with accessibility or special student needs related to platform navigation.
- **secretariat@digital4security.eu** – for questions concerning your student data.

If you ever feel unsure about the next step or experience any technical difficulties, support is just a message away.

Also good to know: The entire platform is compliant with the General Data Protection Regulation (GDPR). A designated Data Protection Officer (DPO) at each partner institution oversees compliance and privacy policies.

15. Welcome Module: Your Launchpad for Success

Before your formal coursework begins, we invite you to start your journey with the **Welcome Week,** during which you actively engage with the **Welcome Module**: your personal launchpad into the master's programme. Whether you are returning to education or new to online study, this self-paced module is designed to help you build confidence, establish routines, and connect with the Digital4Security community from day one.

15.1 What You Will Gain in the Onboarding Module

The Welcome Module supports you in:

- **Mastering the tools**: Learn how to use Moodle, Full Fabric, and other key platforms with ease.
- **Meeting your community**: Get to know your programme directors, instructors, peers, and the partner institutions behind your degree.
- **Navigating the essentials**: Explore your Student Handbook, Module Handbook, and key regulations with step-by-step guidance and short explainer videos.
- **Building sustainable habits**: Discover how to design effective study environments, manage your time, and balance your studies with life and work.
- **Understanding academic integrity**: Learn how to evaluate sources and properly reference both human- and AI-generated content.

15.2 Mindfulness for Online Learning

A unique highlight of the module is the *Mindfulness for Online Learning* series, which provides:

- Research-backed strategies to thrive in remote education
- Tips to enhance creativity, reduce stress, and boost motivation
- Insight into how your environment, mindset, and habits influence success
- Tools and scales to help monitor and support your mental and physical well-being

Whether you are a structured planner or an intuitive learner, these resources will help you build a rewarding and resilient learning experience tailored to your personal style.

15.3 Practical Resources at Your Fingertips

The Welcome Module includes:

- Curated video guides and welcome messages from partners across Europe
- Templates and checklists for organising your academic life
- A growing collection of free well-being and study resources for online learners
- Pointers to optional programmes such as *Career Weeks* and soft skill workshops
- A collection of official programme documents, such as the Student Handbook, the Study and Exam Regulations, the Module Handbook, and more
- Digital4Security templates for your slides, homework submissions, and thesis
- Inspirational mottos, D4S logos, and other branding materials you can use to create custom items (such as T-shirts, mugs, and posters) to express a shared Digital4Security culture and sense of affiliation.

15.4 A Space for Connection and Growth

The Welcome Week is more than a module. It is a space to reflect, connect, and grow. You will have opportunities to:

- Join forum discussions and informal meetups
- Learn about student representation and ways to shape the programme
- Share ideas, questions, and aspirations with the community

Tip: *You can revisit the Welcome Module at any time during your studies. It remains available throughout your programme. Many students return to it regularly for inspiration, resources, or to reset their study habits.*

16. Graduation

Upon successful completion of the Master's Programme, you will be awarded a degree in **Cybersecurity Management and Data Sovereignty**. This section provides an overview of the requirements you need to fulfil for graduation – and how you can celebrate this important milestone together with your peers, instructors, and the wider community.

16.1 Graduation Requirements

To successfully complete the master's programme and be awarded the joint degree, students must meet all of the following academic and administrative requirements:

- 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.

Students who have met all of the above criteria will be eligible to graduate and receive the officially awarded joint degree, conferred by UDS, MTU and UNIR.

If you are unsure about your academic status or progression, we encourage you to contact your **Programme Coordinator** (if you are enrolled in a professional pathway) or reach out to the **Secretariat** at **secretariat@digital4security.eu** for guidance.

16.2 Graduation Ceremony

Graduation marks a significant milestone in your academic and professional journey, and we recognize the importance of celebrating this achievement in a meaningful way. As a fully online joint degree programme, we are committed to offering inclusive options for all students, regardless of their location.

All graduates are invited to participate in an **online graduation ceremony**, ensuring that every student can be recognised and celebrated within our international community. This online ceremony is designed to be a formal and festive occasion, offering graduates the chance to connect with peers, academic staff, and their families in a virtual setting.

However, we also understand that for some students, the **experience of an in-person celebration** is deeply valued. Where possible, the awarding universities may offer opportunities to attend **onsite graduation ceremonies**, subject to availability and institutional scheduling. Participation in such onsite events may require advance registration and may be subject to participation fees and limited space.

For example, **Universidad Internacional de La Rioja (UNIR)** regularly organises **formal graduation events in Spain**. These events are vibrant and well-attended, offering a traditional academic celebration in a physical setting (see Figure 12).

Figure 12: Even after a fully online study experience, celebrating graduation at a festive on-site event can be a meaningful milestone for participants, as illustrated by UNIR.

Attending an onsite graduation ceremony is an optional additional experience and celebration. It does not affect the formal conferral of your degree certificates, which will be issued via the Digital4Security platform in accordance with the joint programme's official procedures.

We encourage all students to participate in the graduation format that best reflects their personal preferences and circumstances.

16.3 After Graduation – Benefit from the Alumni Network

Graduates of the Master's in Cybersecurity and Data Sovereignty are **eligible to join the programme's Alumni Network**, a vibrant community of professionals with experience across business, law, technology, compliance, and related sectors. Alumni membership is flexible: graduates can choose the level of communication and engagement they wish to receive.

The Alumni Network offers opportunities to:

- **Maintain and expand professional connections** with peers and faculty from across Europe and beyond.
- **Participate in exclusive events, workshops, and industry briefings** designed to keep members at the forefront of developments in cybersecurity and data governance.
- **Access continuous learning resources**, including updates on emerging threats, regulatory changes, and best practices in cybersecurity management.
- **Collaborate on professional projects or mentoring initiatives** that connect current students with alumni expertise.
- **Contribute to programme development**, for example through participation in the annual *Future of Learning Convention*, where alumni share insights from their experiences and help shape innovative improvements.

One year and five years post-graduation, alumni will be invited to provide feedback through follow-up surveys to reflect on their experiences and the impact of the programme on their careers.

Joining and staying active in the Alumni Network is straightforward: graduates can register via the programme platform, update their contact preferences, and choose how they wish to receive information and invitations to events. Participation is voluntary but highly encouraged, as it fosters ongoing professional development, strengthens networks, and helps shape the future of the programme.

17. Practical Info

This section offers guidance on practical matters such as working alongside your studies, mobility support, and what is or is not included in your tuition fees. Brief video explainers are also available in the **Welcome Module**.

If you have any further questions, feel free to contact **studyaffairs@digital4security.eu** for additional guidance.

17.1 Working alongside Your Studies

Students in this master's programme may choose to work while studying, and the programme is designed to make that possible. With its **flexible, fully online structure**, modular design, and part-time options, the programme is well-suited to professionals seeking to upskill or transition into new cybersecurity roles without pausing their careers.

That said, if you plan to work during your studies, it is essential to understand and respect the **legal regulations in your country of residence or host country**.

For example, in **Germany**, students are generally permitted to work only **full-time during official term breaks**. During the teaching period, student employment is typically limited to **20 hours per week** to maintain student status and comply with immigration and social security rules.

While the programme offers the flexibility to support working learners, **it is your own responsibility to research and comply with local laws**, including regulations concerning student work permits, taxation, and working hours.

The **term breaks of this programme** are officially defined in the academic calendar (Section 3.9). These breaks typically occur as follows:

- **Spring Break:** Weeks 13-14
- **Summer Break:** Weeks 27-39
- **Winter Break:** Week 52

Working full-time during these breaks is generally less restricted in countries such as Germany, but again – **you must confirm and follow the legal framework applicable to your specific location and visa status**.

If you need guidance on balancing your studies and professional responsibilities, counselling is available via
✉ **studyaffairs@digital4security.eu**.

If you are looking for internship opportunities, career coaching, or job placement support, you can also reach out to
✉ **studyaffairs@digital4security.eu**.

17.2 Fees, Mobility & Support

The **Digital4Security Master's Programme** opens the door to a truly international learning experience, with flexibility, mobility, and real-world opportunities built into the design.

Here is what your tuition fee includes, and what it does not include, along with the types of support available to help you benefit from cross-border collaboration and optional on-site experiences.

17.2.1 What is Included in Your Tuition Fee

Your tuition fee gives you access to the full academic and professional framework of the master's programme. You can complete the full **60 ECTS** curriculum, including:

- **30 ECTS of fixed courses**, made up of:
  - **15 ECTS in mandatory modules**, with one delivered by each awarding university (UDS, MTU, UNIR)
  - **15 ECTS for your thesis**, including academic supervision and assessment
- **30 ECTS of electives**, with:
  - 15 ECTS of **recommended modules** aligned with selected professional profiles (optionally)
  - 15 ECTS of **freely chosen electives**, allowing you to shape your own learning pathway

Furthermore, you can take **industry certification exams** at special rates, with access to self-study materials and mock tests designed to help you succeed.

You will also be invited to a wide range of activities, including:

- Guest lectures, expert webinars, and interactive workshops
- Cybersecurity challenges, cyber ranges, hackathons, and bootcamps
- Networking events, problem-solving projects, and career-building opportunities

While virtual participation in these extracurricular activities is typically free of charge, **some special events may involve a small participation fee** to help cover organisational costs.

Throughout the programme, you benefit from **ongoing student mentoring and formative feedback**, helping you to stay on track and succeed in your studies.

You have access to the full range of **student services** described in this handbook (Section 10).

17.2.2 What is *Not* Included in Your Tuition Fee

While the programme covers a wide range of learning and support services, the following **personal and logistical expenses are not included**:

- Visa or residence permit fees
- Social security or health insurance
- Travel or local transportation
- Housing and lodging costs
- Meals and daily living expenses

These are your personal responsibility. But don't worry, **support is available to help you participate in physical mobility opportunities** (see examples in Section 17.3).

17.3 Student Mobility Support

Whether you join remotely or visit a partner institution in person, we invite you to participate in optional **international activities**, either virtually or on-site. To support this, the programme offers:

- **Letters of invitation to support visa applications**, where needed, for attending on-site events such as summer schools, hackathons, or workshops.
- **Assistance with Erasmus+ applications**, for short-term stays or blended mobility activities
- **Local mobility services** offered by selected partner universities

Here is one example: Local Support at UDS (Germany)

Students enrolled in this Master's programme are eligible to take part in **Career Weeks** in Germany: an optional, four-week immersive experience organized by UDS that brings your online studies to life. Hosted at the CloudHouse headquarters in Potsdam (near Berlin), the programme offers:

- **Hands-on career development workshops** covering professional skills, case studies, and career coaching
- **Short-term internships and onsite networking events**, connecting you directly with industry professionals in the region
- **Support finding affordable housing** in the Berlin–Potsdam area
- **Access to UDS's CloudHouse facilities** for workshops and collaborative learning
- **Cultural activities** such as museum visits and boat tours
- **Community-building events** around Potsdam and Berlin
- **Tailored assistance with travel and logistics**, designed around your individual goals

For more information, visit **www.germanuds.de/careerweeks**.

This is just one example. Many other Digital4Security partner institutions may also offer mobility support, including help with internships, physical events, or local services for international students.

18. Branding and Shared Culture

At many on-site universities, students and visitors can buy branded t-shirts, cups, and pens – often as a way to express affiliation, pride, or a sense of belonging to a shared community and culture. These items can become meaningful keepsakes, even for alumni or family members.

We fully support the desire to express a shared culture. In an online programme with partners across multiple European countries, our diversity, mutual respect, and spirit of collaboration form a core part of this identity.

In the **Welcome Module** materials, you will find a collection of resources that can be downloaded **for free**. You can use them to create your own branded items, such as t-shirts, mugs, or stationery. This allows you to feature the designs and messages that resonate most with you. For the printing and customization, you can choose retailers of your preference, such as local companies.

Available resources include:

- The D4S logo and branding assets, including materials linked to the D4S network, the involved institutions and the diversity of European locations;
- Inspirational quotes and mottos on cybersecurity, risk management, and innovation governance – ideal for printing on banners to customize your home environment;
- D4S academic templates, including slides and thesis support materials for structuring and presenting your work.

We warmly invite you to explore and personalise these materials to reflect your own style and ideas. Feel invited to share how you have integrated D4S elements into your environment, clothing, or everyday items. We have a dedicated forum in

the **Welcome Module** where you can post your creations, share inspiration, and celebrate the shared values of the D4S community.

19. Key Contacts

For all general enquiries and support, the Digital4Security team is here to help. Below you will find dedicated contact points for common questions and concerns throughout your studies.

19.1 General Support

General Enquiries
For questions about the programme, how it works, and who to contact.
✉ **studyaffairs@digital4security.eu**

Student Services
For help in navigating your studies or accessing student support services
✉ **studyaffairs@digital4security.eu**

19.2 Admissions and Enrolment

Admissions Office
For questions about applications or entry requirements
✉ **online.admissions@digital4security.eu**

Student Data and Records
For help with student IDs, transcripts, and your profile data.
✉ **secretariat@digital4security.eu**

19.3 Programme Governance and Academic Support

Programme Secretariat
For matters related to day-to-day programme operations, scheduling, and coordination.
secretariat@digital4security.eu

Programme Coordinators
For questions concerning the programme, any operational concerns or suggestions
Programme Coordinator – UDS
coordinator.uds@digital4security.eu

Programme Coordinator – MTU
coordinator.mtu@digital4security.eu

Programme Coordinator – UNIR
coordinator.unir@digital4security.eu

19.4 Quality, Feedback, Conflict-Guidance

I Like – I Wish – Clarify
Use this channel to submit feedback or suggestions.
quality.committee@digital4security.eu

Quality Assurance
To contact the Quality Service Committee.
quality.committee@digital4security.eu

Ombudsperson
For confidential guidance around conflicts, unfair treatment, or appeals.
ombudsperson@digital4security.eu

19.5 Formal Complaints

When informal channels do not suffice to solve issues, contact the programme coordinators.

Programme Coordinator – UDS

coordinator.uds@digital4security.eu

Programme Coordinator – MTU

coordinator.mtu@digital4security.eu

Programme Coordinator – UNIR

coordinator.unir@digital4security.eu

19.6 Student Representation

Contact Your Student Representatives

To reach out to elected representatives for concerns, suggestions, or support.

studentreps@digital4security.eu

19.7 Career Services and Industry Certifications

Employability and Internship Support

For internship or job placements, or information on industry certifications, including support with mock exams and recommended certifications.

studyaffairs@digital4security.eu

19.8 Professional Profiles and Pathway Support

For questions regarding a certain professional pathway and its recommended modules, contact the Programme Coordinator of the curating institution

Chief Information Security Officer (CISO)
Programme Coordinator – UDS
coordinator.uds@digital4security.eu

Cyber Legal, Policy, and Compliance Officer
Programme Coordinator – MTU
coordinator.mtu@digital4security.eu

Cybersecurity Risk Manager
Programme Coordinator – MTU
coordinator.mtu@digital4security.eu

Cyber Threat Intelligence Specialist
Programme Coordinator – UNIR
coordinator.unir@digital4security.eu

Cybersecurity Educator
Programme Coordinator – UDS
coordinator.uds@digital4security.eu

Cybersecurity Auditor
Programme Coordinator – UNIR
coordinator.unir@digital4security.eu

19.9 Additional Contacts

IT Helpdesk

For platform issues, login problems, or system access.

IT@digital4security.eu

Event and Community Coordination

For events, workshops, or networking opportunities.

studyaffairs@digital4security.eu

Glossary of Terms

Academic and Programme Terms

- **ECTS (European Credit Transfer and Accumulation System)**

A standardized system across Europe that measures student workload. 60 ECTS credits represent a full-time academic year.

- **Programme Learning Outcomes (PLOs)**

Broad competencies and skills that students are expected to achieve by the end of the degree programme.

- **Module Learning Outcomes**

Specific knowledge and skills students should acquire by completing a particular module.

- **Module Catalogue**

A list of all modules available in the programme, including descriptions, credit value, and relevance to professional profiles.

- **Module Guarantor**

The institution responsible for ensuring academic quality and oversight of a specific module.

- **Diploma Supplement**

An official document accompanying the degree that details academic achievements, modules completed, and professional pathway alignment.

- **Joint Degree**

A single degree awarded by multiple institutions, recognizing joint delivery and oversight of the programme.

- **Trimester**

An academic term structure dividing the year into three periods of approximately 12 weeks each.

- **Programme Coordinator**

The staff member responsible for overseeing a student's academic journey and ensuring alignment with their chosen professional profile.

- **Professional Profile / Pathway**

A curated learning track aligned with specific cybersecurity career roles, offering tailored guidance and documentation.

- **Elective Module**

A module chosen by the student based on interest or professional goals, not compulsory for all.

- **Mandatory Module**

A required module that all students in the programme must complete.

- **Micro credential**

Short, focused learning experiences that can be recognized for credit towards a degree.

- **Recognition of Prior Learning**

A process for acknowledging previous formal or informal learning to gain academic credit.

- **Transcript of Records**

An official document listing all modules completed, ECTS earned, and grades achieved.

- **Welcome Module**

An onboarding module that helps students navigate the programme, platform, and study expectations.

- **Learning Management System (LMS)**

The digital platform used to deliver course materials, assignments, and communication (e.g., Moodle).

Cybersecurity-Specific Terms

- **Cybersecurity Management**

The strategic oversight of an organisation's information security policies, practices, and risk management.

- **Data Sovereignty**

The concept that digital data is subject to the laws of the country in which it is stored.

- **Ethical Hacking**

The practice of testing systems and networks to identify vulnerabilities, performed legally and with consent.

- **Penetration Testing**

Simulated cyberattacks on systems to evaluate their security resilience.

- **Cyber Threat Intelligence**

Information gathered and analysed to understand potential and active threats to an organisation's digital assets.

- **Cyber Risk Management**

The process of identifying, evaluating, and mitigating risks to digital infrastructure and data.

- **Cybersecurity Operations**

Day-to-day activities involved in detecting, responding to, and preventing cybersecurity incidents.

- **Cybersecurity Auditor**

A professional who assesses an organisation's cybersecurity posture, compliance, and risk exposure.

- **Cybersecurity Law**

Legislation governing digital security practices, privacy, data protection, and compliance.

- **Digital Forensics**

The investigation of digital devices and data for evidence in cybersecurity and legal contexts.

- **Cyber-Physical Systems**

Integrated systems involving both digital and physical components, such as industrial control systems.

- **Security Operations**

Organisational functions focused on monitoring, managing, and securing digital infrastructure.

- **Incident Management**

The process of identifying, responding to, and recovering from cybersecurity incidents.

- **Malware Analysis**

The study of malicious software to understand its function, origin, and impact.

- **CISO (Chief Information Security Officer)**

An executive responsible for an organisation's information and cybersecurity strategy.

- **Chain of Custody**

The documented process of handling digital evidence to maintain its integrity.

- **eDiscovery**

The process of identifying, collecting, and producing digital data in response to a legal request.

- **Cybersecurity Culture**

The shared values, practices, and awareness around information security within an organisation.

- **Cybersecurity Strategy**

A long-term plan that outlines how an organisation will protect its information assets.

- **Compliance**

Adherence to relevant laws, regulations, and standards.

- **Governance**

Structures and policies that define how cybersecurity responsibilities are managed and overseen.

- **Threat Response**

Actions taken to address and mitigate identified cyber threats.

Governance Terms

- **Academic Integrity**

A commitment to honesty, trust, fairness, respect, and responsibility in academic work, including avoiding plagiarism and cheating.

- **Appeals Process**

A formal procedure allowing students to contest academic decisions, such as grades or admissions outcomes.

- **Code of Conduct**

A set of rules outlining expected behaviours and responsibilities of students within the academic community.

- **Student Representation**

A governance structure that allows students to participate in decision-making and voice concerns to programme leadership.

- **Disciplinary Procedures**

Processes for addressing breaches of institutional rules or academic misconduct.

- **Ombudsperson**

An impartial official who assists students in resolving disputes or concerns within the academic institution.

- **Document Hierarchy**

The structured relationship between policy documents, with legal and institutional documents taking precedence over others.

Digital Tools and Platforms

- **Moodle**

An open-source Learning Management System (LMS) used for delivering course content, assignments, and communication.

- **Full Fabric**

A digital platform used to manage applications, student profiles, and admissions.

- **Cyber Ranges**

Simulated environments used for cybersecurity training and exercises, allowing learners to practice in realistic scenarios.

- **Immersive Learning**

Learning experiences enhanced through digital simulations, 3D environments, or augmented/virtual reality technologies.

- **Cloud Computing**

The delivery of computing services such as storage, processing, and software over the internet.

- **Automation of Security Tasks**

The use of software tools and scripts to automatically perform security operations and threat detection tasks.

- **Machine Learning**

A type of artificial intelligence that enables systems to learn and improve from experience without explicit programming.

- **Deep Learning**

A subset of machine learning using neural networks with multiple layers, often used in cybersecurity for threat detection.

Quality Assurance Terms

- **Quality Assurance**

A systematic process of monitoring and improving academic standards and student learning outcomes.

- **Internal Quality Handbook**

A document outlining how the programme maintains academic quality through feedback, monitoring, and evaluation.

- **Accreditation**

Official recognition that an academic programme meets defined quality standards set by a regulatory or accrediting body.

- **Continuous Monitoring**

Ongoing assessment of programme performance, including teaching quality, student satisfaction, and learning outcomes.

- Fe**edback Mechanisms**

Structured processes through which students can provide input on modules, teaching, and services to help improve the programme.

- **'I Like, I Wish, Clarify'**

A structured feedback method encouraging constructive input from students: what they liked, wished for, or found unclear.

Acronyms – Academic and Programme Terms

- **ECTS**

European Credit Transfer and Accumulation System – already defined.

- **LMS**

Learning Management System – a software application for the administration, documentation, tracking, reporting, automation, and delivery of educational courses.

- **CEFR**

Common European Framework of Reference for Languages – used to define and measure language proficiency.

- **EQF**

European Qualifications Framework – a standardised system for comparing qualifications across Europe.

- **EHEA**

European Higher Education Area – a unified higher education framework in Europe enabling degree recognition and academic mobility.

Acronyms - Economy and Cybersecurity

- **SMEs**

Small and Medium-sized Enterprises.

- **CPS**

Cyber-Physical Systems – integrated systems involving computation, networking, and physical processes.

Acronyms – Digital Tools and Platforms

- **COVE**

Campus of Virtual Education – a digital space used for immersive learning.

- **D4S**

Digital4Security – an EU-funded project supporting cybersecurity education across Europe.

Acronyms – Governance Terms

- **UNESCO**

United Nations Educational, Scientific and Cultural Organization.

- **CEPES**

European Centre for Higher Education (part of UNESCO).

Document Governance

This **Student Handbook** is a shared programme resource, overseen by the Master's Board and operationally managed by the Secretariat, as defined in the *Cooperation Agreement* (Annex 1). Content revisions and quality checks are carried out with the support of the Quality Service Committee and the Industry Advisory Board. Together, these bodies ensure that the handbook is accurate, comprehensive, and aligned with the programme's policies, procedures, and standards.

The Quality Service Committee supports the Secretariat in ensuring that the handbook accurately reflects the programme's policies and covers all essential programme information.

The Industry Advisory Board helps to ensure that students can readily access information relevant to professional career goals, with opportunities offered through the Digital4Security partner network clearly highlighted.

All **Digital4Security partners** are invited and encouraged to suggest additional services, information or resources for inclusion in the handbook. Once approved by the Master's Board, these contributions will be added, helping connect students with partners who provide valuable expertise and opportunities.

The handbook is designed to empower learners, supporting them in navigating the digital learning environment with confidence and enabling them to make the most of the programme from the outset.

Submitting Suggestions or Feedback

- Partners, staff, and programme bodies are encouraged to propose enhancements to the handbook, whether through revisions or the addition of new content.
- Students are invited to provide feedback, for example if sections are unclear or if additional information would be useful.

- Suggested edits should be sent to **secretariat@digital4security.eu**, with **quality.committee@digital4security.eu** copied (Cc).
- For internal consultation on potential new contributions – before suggesting concrete edits, discussions may be directed to:
    - the Industry Advisory Board (**advisory-board@digital4security.eu**) for proposals by Industry Partners, or
    - the Quality Service Committee (**quality.committee@digital4security.eu**) for proposals by Academic Partners.

Updating the Handbook

- The Secretariat implements changes, with guidance and editorial support from the Quality Service Committee.
- Substantial content changes require the approval of the Master's Board.
- Once a new version is authorised, the Secretariat will publish it on the designated platforms without undue delay. All programme participants and affiliates will be notified through official channels within two weeks of the revision.

The current document is designated as *Student Handbook, Version 1 (V1)*. Editorial changes, such as correcting spelling errors or updating figures without altering 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

This **Student Handbook** forms 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	✓	✓	(✓)
7	Module Handbook	✓	✓	(✓)

No.	Document	SharePoint	Welcome Module	Website
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.

Legal Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HaDEA). Neither the European Union nor the granting authority can be held responsible for them.

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