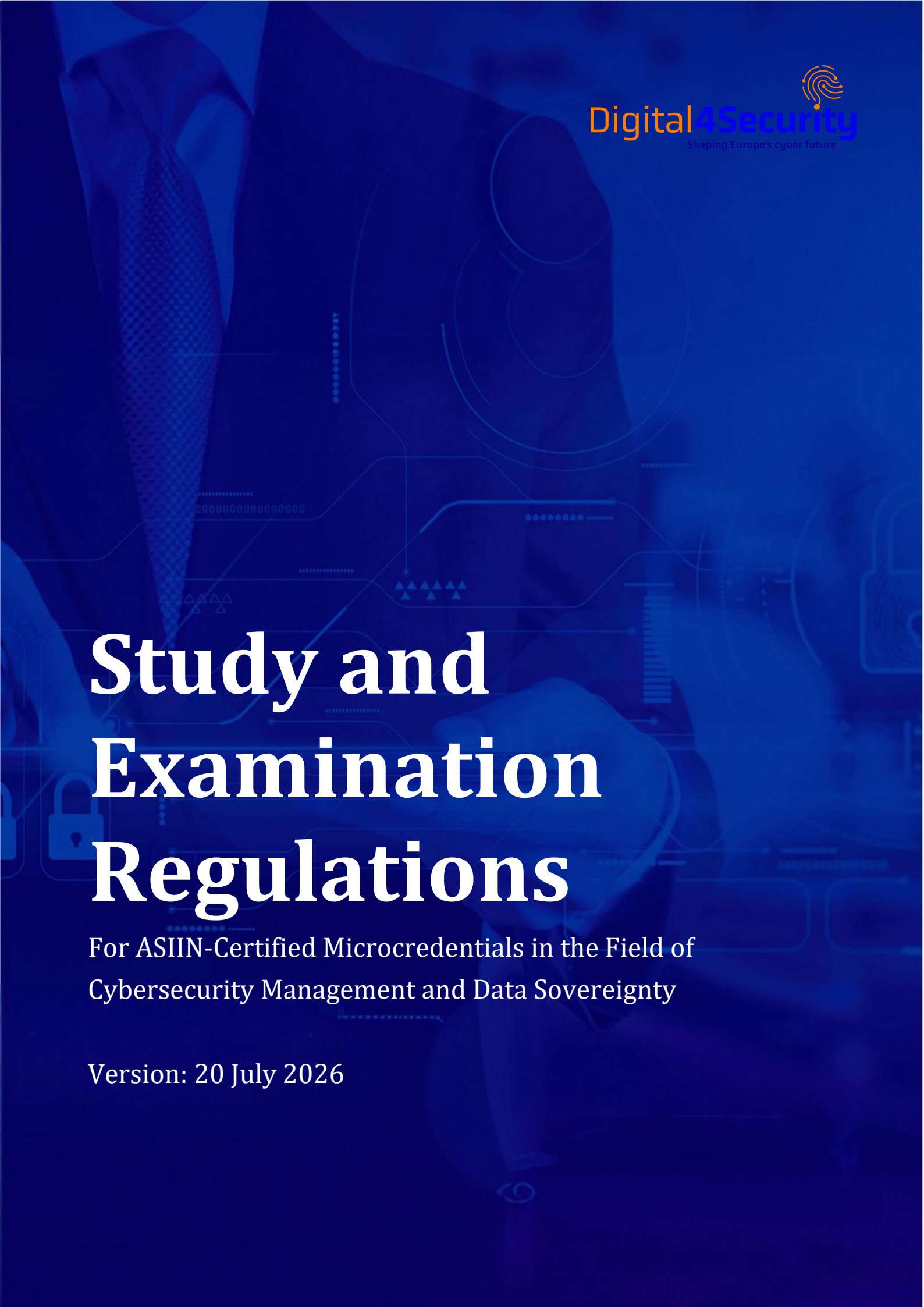

Digital4Security
Shaping Europe's cyber future

Study and Examination Regulations

For ASIIN-Certified Microcredentials in the Field of Cybersecurity Management and Data Sovereignty

Version: 20 July 2026

Table of Contents

1. Introduction

1.1 Microcredentials, Modules, and ASIIN Certification

These *Study and Examination Regulations* govern ASIIN-certified microcredentials awarded by the German University of Digital Science (UDS) and delivered in collaboration with partners from across the Digital4Security network. All modules support learning in the broad field of **Cybersecurity Management and Data Sovereignty**.

A **microcredential** is a focused, credit-bearing learning offer that enables learners to develop specific knowledge, skills, and competences within a clearly defined subject area. Unlike a full degree programme, a microcredential concentrates on a more specific area of study and can normally be completed within a comparatively short period of time.

Across the learning offers governed by these *Study and Examination Regulations*, each microcredential corresponds to a single academic **module**. They are defined in terms of specific learning outcomes, teaching and learning activities, assessment requirements, workload, and ECTS credits in accordance with the **European Credit Transfer and Accumulation System** (ECTS).

The modules are worth **5 ECTS** credits each, corresponding to an overall learner workload of approximately **125 hours**. They are designed to be completed over a period of **12 weeks**, with an average study workload of around 10 hours per week. All microcredentials are positioned at **Level 7** of the **European Qualifications Framework** (EQF), corresponding to Master's-level academic standards.

Microcredentials are designed to be studied individually and flexibly, independent of a full degree programme. They allow learners to develop selectively those competences that are most relevant to their current professional responsibilities or future career aspirations.

Across Europe, many higher education institutions increasingly recognise successfully completed microcredentials as prior learning within Bachelor's, Master's, or

doctoral programmes, potentially reducing the volume of study still required towards the respective qualification. In this context, recognition decisions remain subject to the applicable national, regional and institutional regulations. Learners intending to use completed microcredentials towards another qualification are therefore advised to consult the admission and recognition policies of the respective programme.

The **ASIIN certification** confirms that the modules governed by these *Study and Examination Regulations* have successfully undergone independent external quality assurance. It demonstrates that these learning offers satisfy internationally recognised standards with regard to academic level, Intended Learning Outcomes, curriculum design, assessment, quality assurance, and transparency. This supports the credibility, comparability, and international recognition of the awarded microcredentials.

These *Study and Examination Regulations* define the academic and procedural framework applicable to learners enrolled in the ASIIN-certified microcredentials awarded by UDS and delivered in collaboration with partners from the Digital4Security network. They establish the rules governing admission, participation, assessment, grading, re-assessment, academic integrity, appeals, and certification. They provide a **binding framework** for all parties involved in the ASIIN-certified microcredentials, including learners, educators, administrators, and those responsible for quality assurance.

Upon successful completion of a microcredential, learners receive an official **certificate issued by the German University of Digital Science** documenting the title of the completed learning offer, the achieved learning outcomes, the awarded ECTS credits, the corresponding qualification level and other constitutive information required for transparent academic recognition.

1.2 About the Digital4Security Project

The development and delivery of ASIIN-certified microcredentials is supported through **Digital4Security**, a project co-funded by the European Union under the DIGITAL Europe Programme (Grant Agreement No. 101123430; DIGITAL-2022-SKILLS-03 – Advanced Digital Skills). Through this European initiative, higher education institutions, research organisations, employment services, industry partners, and other stakeholders contribute academic expertise, professional perspectives, and shared resources to support the development and delivery of flexible, high-quality, and market-relevant cybersecurity education.

The Digital4Security project aims to strengthen advanced cybersecurity education across Europe by developing innovative and sustainable learning opportunities in the fields of Cybersecurity Management and Data Sovereignty. The project responds to the growing demand for cybersecurity professionals by combining academic excellence with practical and industry-relevant perspectives.

The consortium brings together higher education institutions and associated partners from across Europe. Table 1 provides an overview of the organisations participating in the Digital4Security network.

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	BUT	Czech Republic	HEI partner

No.	Partner	Abbreviation	Country	Role
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 CERGY	France	HEI partner
11	Cyber Ranges Ltd	CYBER RANGES	Cyprus	Associate partner
12	DigitalEurope AISBL	DIGITALEUROPE	Belgium	Associate partner
13	Digital Technology Skills Limited	DTSL	Ireland	Associate partner
14	European Digital SME Alliance	DIGITAL SME	Belgium	Associate partner
15	Fraunhofer Gesellschaft zur Förderung der Angewandten Forschung EV	FHG	Germany	Associate partner
16	German University of Digital Science	UDS	Germany	HEI partner
17	Independent Pictures Limited	INDIEPICS	Ireland	Associate partner
18	IT@Cork Association Limited LBG	IT@CORK	Ireland	Associate partner
19	Matrix Internet Applications Limited	MATRIX	Ireland	Associate partner
20	Munster Technological University	MTU	Ireland	HEI partner
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

No.	Partner	Abbreviation	Country	Role
30	Skillnet Ireland Company Limited By Guarantee	SKILLNET	Ireland	Associate partner
31	Terawe Technologies Limited	TERAWE	Ireland	Associate partner
32	Universidad Internacional de La Rioja	UNIR	Spain	HEI partner
33	Università degli Studi di Brescia	UNIBS	Italy	HEI partner
34	Universitatea Națională de Știință și Tehnologie Politehnica București	UPB	Romania	HEI partner
35	Universität Koblenz	UNI KO	Germany	HEI partner
36	University of Rijeka	UNIRI	Croatia	HEI partner
37	Vytautas Magnus University	VMU	Lithuania	HEI partner

Together, the partner organisations contribute to a shared European ecosystem for cybersecurity education. Learning offers developed within the project benefit from common academic and industry expertise as well as shared digital infrastructure. The latter includes a common Learning Management System (based on Moodle) and a Customer Relationship Management system (based on Gibbon), together with additional resources and services that support the design, delivery, and administration of the learning offers.

While all Digital4Security learning offers benefit from the insights, infrastructure, and resources developed through the EU co-funded project, each academic offering is designed to be self-contained and sustainable beyond the project's funding period.

2. Admission Requirements

Applications for admission to an ASIIN-certified microcredential are submitted via the centralised online application portal, accessible through the Digital4Security website at **www.digital4security.eu**. Applications and enrolment are possible three times per year, with modules commencing in January, April, and October.

2.1 Minimum Entry Requirements

The microcredentials are designed to support accessible, flexible, and lifelong learning. To minimise unnecessary barriers to participation, no formal academic qualifications or prior educational certificates are required for admission. Instead, the modules are open to all eligible learners who consider themselves sufficiently prepared to participate successfully. Applicants are therefore expected to assess for themselves whether they meet the participation requirements. During the application process, they must confirm by means of a self-declaration that they:

- possess sufficient English language proficiency to participate effectively in a learning offer delivered in English.
- have reliable access to the technical equipment and internet connection required for online study.
- have read the module description, including, where applicable, any specified prerequisite knowledge, and that they possess such prerequisite knowledge where required.

2.2 Necessary Documentation for Application

All applications must be submitted via the programme's online application portal in accordance with the published deadlines and instructions. A complete application must include a copy of the applicant's valid passport, national identity card, or other accepted travel document. It must clearly indicate the applicant's full name, date of birth, citizenship, and the document's validity period.

Applicants must also confirm their English language proficiency, access to the technical resources required for online study, possession of any specified prerequisite knowledge where relevant, and acceptance of the **General Terms and Conditions**.

By submitting an application, applicants confirm that all information and documentation provided are accurate, complete, and up to date. They further consent to the processing of their personal data for the purposes of administering the admission process and their participation in the learning offer.

2.3 Language Qualification Requirements

As the learning offers are delivered in English, applicants must confirm that they possess sufficient English language proficiency to participate effectively in teaching, collaborative learning activities, and assessments.

2.4 Required Equipment

To successfully participate in online study, learners must ensure access to essential equipment and infrastructure. The following equipment is required:

- **Laptop or Desktop Computer, or equivalent:** Capable of running video conferencing tools, accessing cloud-based learning platforms, and using standard productivity software.
- **Internet Connection:** Stable and fast enough to stream lectures, join live seminars, and upload assignments.
- **Webcam and Microphone:** Required for oral assessments and interactive sessions.
- **Controlled Study Environment for Exams:** During assessments, learners may have to ensure that they are in an interruption-free space where no individuals, animals, or objects can enter or interfere in an uncontrolled manner.

2.5 Application Review Procedure

Admission decisions are made by UDS, supported by the Digital4Security partner network, where applicable.

Admission may be refused where an applicant does not meet the published eligibility requirements, where required documentation or payment has not been provided, where the available number of places has been reached, or where further restrictions apply, for example under the applicable rules governing an EU co-funded project.

The University reserves the right to verify the authenticity of submitted documentation and to refuse admission, revoke an offer of admission, or cancel enrolment where false, misleading, expired, or otherwise invalid documentation has been submitted.

Where admission is refused after payment has been made, any fees received shall be refunded to the applicant without undue delay, unless otherwise explicitly agreed for separate services.

2.6 Rejection Appeals

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

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

3. Governance of ASIIN-Certified Microcredentials

The organisational structure of ASIIN-certified microcredentials follows the framework established in the Digital4Security **General Terms and Conditions**. In particular, responsibilities are divided between the **Awarding Partner** and the **Delivering Partner**. These roles are defined as follows:

- - - Excerpt from the General Terms and Conditions (Definitions) **- - -**

Awarding Partner means the higher education institution responsible for the academic governance of a Learning Offer and for awarding the qualification upon its successful completion by the participant.

The Awarding Partner is responsible for ensuring that the Learning Offer complies with the applicable legal and academic requirements, including quality assurance. Unless expressly stated otherwise in the applicable Product Information, any contractual relationship established through enrolment in a Learning Offer is concluded between the participant and the Awarding Partner.

Delivering Partner means an institution making substantial academic contributions to the design and/or delivery of a Learning Offer.

The Delivering Partner will ordinarily be the institution with which participants primarily interact during the Learning Offer through teaching, learner support, assessment activities or other educational services.

- - -

The division of responsibilities set out in the General Terms and Conditions also applies to the ASIIN-certified microcredentials. In addition, the following provisions apply.

The responsibilities of the Awarding Partner further include:

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

The review and approval of learning materials and assessments shall normally take place no later than one month before the start of the module. This may be implemented either through a review of the module prepared by the Delivering Partner by an authorised representative of the Awarding Partner, or through a peer review between different Delivering Partners, conducted in accordance with the Awarding Partner's standard review template.

The **Awarding Partner can be contacted** by email at:
coordinator.uds@digital4security.eu.

The responsibilities of the Delivering Partner further include:

- preparing, maintaining, and delivering the module, including its learning materials and assessments, in accordance with the *Module Handbook*, these *Study and Examination Regulations*, and the applicable quality assurance requirements, ensuring that all materials are ready for quality assurance review no later than one month before the start of the module;
- allocating lecturers in compliance with these *Study and Examination Regulations*;
- providing academic support to learners throughout the module;
- conducting assessments, grading learner performance, and submitting assessment results to the Awarding Partner within the agreed timelines for review and confirmation;

- cooperating with the Awarding Partner and authorized partners in quality assurance procedures, module reviews, and the implementation of agreed improvement measures; and
- promptly informing the Awarding Partner of any circumstances that may affect the quality or successful delivery of the module, and providing any information reasonably required for its administration, quality assurance, and certification.

Contact details for the Delivering Partner are provided in the module-specific Product Information. Once enrolled and granted access to the module through the Learning Management System, participants are expected to communicate with the Delivering Partner primarily through the platform.

3.1 Assessment and Grading Quality Assurance

The following order of precedence applies: The Awarding Partner is responsible for issuing all grades in the programme. Where applicable, the Awarding Partner confirms the grading procedures and outcomes of the Delivering Partner. The Awarding Partner's Examinations Board oversees all grading processes and may, where appropriate, audit grading procedures and outcomes.

Grading oversight shall focus on the assessment tasks, grading criteria, and grading procedures established for the module, as part of the quality assurance review conducted one month prior to module delivery. Grades duly issued in accordance with the module's confirmed assessment procedures should ordinarily not be altered, unless there is substantiated evidence of academic misconduct affecting the task performance, or there are other significant reasons. All relevant bodies and individuals shall coalesce to ensure that grades displayed on the learning platform are reliable and valid, with oversight systematically addressing all aspects of assessment design and grading, and with final confirmation and issuance of grades taking place in a timely manner.

3.2 Instructor Requirements

The main instructor responsible for delivering an ASIIN-certified microcredential must meet the following minimum requirements:

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

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

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

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

Throughout the entire life cycle of a module, Instructors are expected to build on the guidance provided by the Awarding Partner and the Digital4Security network, and to consult the *Practical Guide for Lecturers* in preparing and delivering their modules.

3.3 Supporting Instructional Quality via Data Analysis

The quality of module delivery is monitored through a systematic, data-informed quality assurance process. The Awarding Partner is responsible for systematically reviewing the available data, identifying any issues requiring follow-up, supporting targeted improvement measures where appropriate, and highlighting exemplary teaching practices. Identified examples of good practice are shared across the teaching team to support continuous professional development.

The Awarding Partner also ensures that relevant good practices and resulting recommendations are progressively incorporated into the *Practical Guide for Lecturers*, an internal guidance document intended to support the design, delivery, assessment, and continuous improvement of programme modules.

4. Period of Study

Study workload is defined using the **European Credit Transfer and Accumulation System** (ECTS). Within the ASIIN-certified microcredentials, **one ECTS credit corresponds to approximately 25 hours of learner effort**, including all study-related activities such as engaging with the learning materials, completing assignments, participating in optional live sessions, and self-study.

Each module within the ASIIN-certified microcredentials comprises 5 ECTS credits, corresponding to an approximate total learner workload of 125 hours. All modules are designed to run over a period of 12 weeks, with an indicative average **study workload of approximately 10 hours per week**.

4.1 Academic Calendar for ASIIN-Certified Microcredentials

The academic year comprises three terms (cf. Figure 1):

- Winter Term (1 January to 31 March)
- Spring Term (1 April to 30 June)
- Autumn Term (1 October to 31 December)

Enrolment is possible for each of these terms.

Where operationally necessary, the start of a 12-week module may be shifted by up to one week relative to the academic term. The exact module start date is specified in the respective module description on the Digital4Security website at **www.digital4security.eu/microcredentials**.

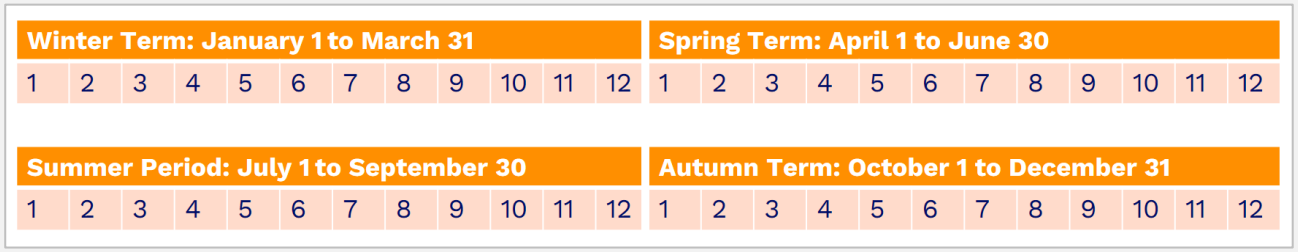

Figure 1: Structure of the academic calendar – three academic terms, each comprising 12 weeks.

4.2 Assessment and Grading Timeline

Final assessments normally take place during the **final two weeks** of the module.

Repeat or re-sit assessments should ordinarily take place during the **first two weeks following the end of the module**.

Final grades are typically confirmed **within eight weeks** following the end of the module.

The Delivering Partner shall submit all assessment results, together with the corresponding final module grade, to the Awarding Partner for review as soon as reasonably practicable following the completion of the module's assessment activities, and no later than four weeks after the end of the module. This serves to ensure that the Awarding Partner, or its authorised reviewers, have at least four weeks to review the submitted assessment results across all ASIIN-certified microcredentials and formally issue the final grades.

During the months from July to September, no regular delivery of ASIIN-certified microcredentials takes place, reflecting the summer vacation schedules observed by several D4S partners. However, UDS remains in regular operation throughout this time. Where reasonably possible, and subject to the timely completion of grading by the Delivering Partner, final grades for modules completed during the Spring Term will therefore also be confirmed within eight weeks following the end of that term.

Figure 2 provides an overview of the assessment and re-assessment timelines across the academic year.

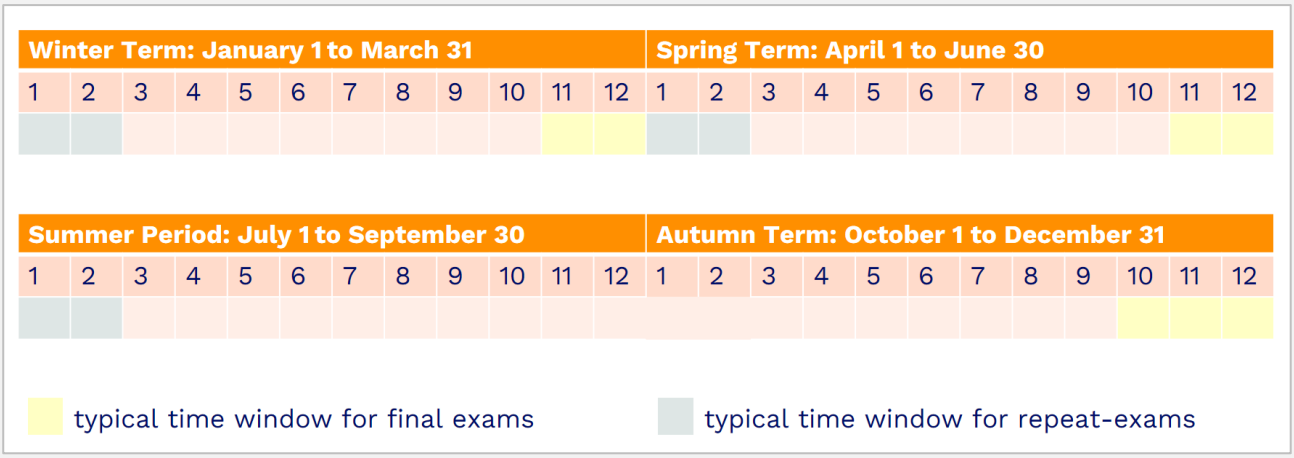

Figure 2: Examination and re-assessment timelines across ASIIN-certified microcredentials.

4.3 Weekly Material Release

Learning materials are normally released on a weekly basis, allowing learners to engage with the content and complete the required learning activities at times during the week that best fit their professional and personal commitments.

4.4 Recommended Standard Module Structure

As Awarding Partner, UDS recommends the following standard structure for ASIIN-certified microcredentials.

- **Pre-Weeks (first two weeks of the term):** These are dedicated to orientation and preparation. For modules specifying prerequisite knowledge, corresponding self-tests and introductory learning materials are provided. Beyond such preparation, further topics may be introduced. Educational resources are provided asynchronously only, with most learning content marked as optional rather than required. Continuous assessments and live sessions do not yet take place.

- **Lecture Weeks (middle eight weeks of the term):** They constitute the core learning phase, during which the main learning activities, continuous assessments, and optional live sessions take place.
- **Post-Weeks (final two weeks of the term):** They are reserved primarily for final submissions and assessments. Where reasonably possible, final assessments should provide learners with flexibility regarding their exact completion time. For example, a final quiz or the submission window for project documentation may remain open throughout the final two or three weeks of the module, allowing learners to complete the assessment at a time that best accommodates their own schedule.

Learning materials are normally released from the Pre-Weeks until the end of the Lecture Weeks, supporting independent study throughout this period. During the Lecture Weeks, continuous assessments also typically take place. During the Post-Weeks, no new learning content is normally introduced. Instead, learners are expected to use this time for revision, completing final examinations, and/or submitting final project work.

A core design principle of the ASIIN-certified microcredentials is to support flexible, self-paced learning. Mandatory learning materials are therefore provided asynchronously through the online learning environment, allowing learners to engage with the module at times that best suit their professional and personal commitments.

During each Lecture Week, learners will typically complete at least one continuous assessment related to the weekly topic and may participate in optional live sessions that provide opportunities to ask questions, seek clarification, and discuss practical applications. Final assessments are normally scheduled during the Post-Weeks or, where appropriate, during the final Lecture Week.

The planned learning materials, activities, and assessments are designed to correspond to an average learner workload of approximately 10 hours per week across the full 12-week term (cf. Figure 3).

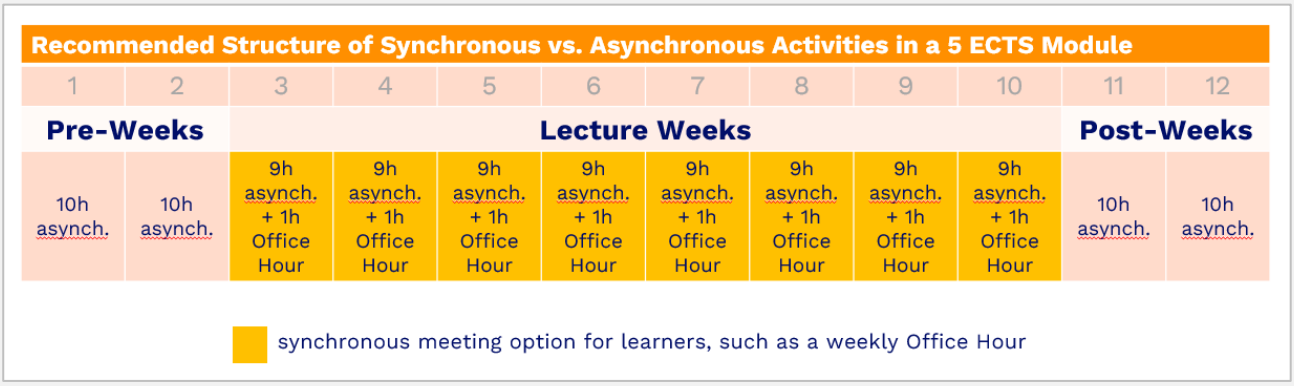

Figure 3: Recommended standard structure of a 12-week module.

As an internal guideline for allocating the recommended average weekly study workload of approximately 10 hours, the distribution shown in Table 2 is recommended for the Lecture Weeks. During the Pre-Weeks, live session time is replaced by additional prepared asynchronous learning materials.

Table 2: Recommended Weekly Time Allocation for a 5 ECTS Module (Lecture Week)

Activity	Approximate Time
Pre-recorded learning materials	1–2 hours
Optional live sessions (recorded where appropriate)	1–2 hours
Core exercises and readings	1–4 hours
Group collaboration, project or lab work (may overlap with core exercises)	Up to 4 hours
Independent exploration (optional)	1–2 hours
Overall weekly workload	**Approx. 10 hours**

Core content should be provided in the form of short, high-quality learning chunks, such as brief videos, also made available as downloadable slides and audio-only versions. As a rule of thumb, individual learning inputs should ideally last around 6–7 minutes and generally not exceed 20 minutes. Accordingly, a weekly teaching input corresponding to approximately one hour of instruction would typically comprise between three to ten short videos or other engaging learning resources. This approach supports flexible learning for working professionals by enabling learning to take place in short, self-contained sessions that can be fitted around professional and personal commitments.

4.5 Live Session Organisation

During the Lecture Weeks, educators are recommended to offer a weekly **Office Hour**. Participation is optional and provides learners with an opportunity to ask questions, seek clarification, or discuss cases from their professional practice in relation to the weekly topic.

Educators may also offer additional live learning activities where appropriate, as specified in the *Module Handbook* with further details provided in the *Basic Course Information*. However, the microcredentials are designed primarily for flexible, self-paced study. Accordingly, all mandatory learning materials shall be provided asynchronously within the online learning environment and may be accessed by learners at their own pace. Live activities are intended to complement, rather than constitute, the core learning experience.

With regard to live sessions, learners are furthermore referred to the data protection provisions set out in the Digital4Security **General Terms and Conditions**. Across the ASIIN-certified microcredentials, **live sessions may be recorded** and made available to participants within the module to support flexible learning, and to enable those unable to attend synchronously to access the relevant content. Learners provide their consent to such recordings by accepting the General Terms and Conditions as part of the admission procedure. Furthermore, as set out in the General Terms and Conditions, recordings are provided exclusively for personal learning purposes within the respective Learning Offer and must not be downloaded, shared, published, or otherwise distributed without prior permission.

4.6 Flexibility Provisions

An important benefit of the Digital4Security initiative is that learners have the opportunity to engage with the cybersecurity expertise, perspectives, and educational practices from leading institutions across Europe. Although the certificate of successful completion for an ASIIN-certified microcredential is awarded by UDS, the overall module portfolio is designed and delivered through an international network of higher education institutions and industry partners.

While the overall structure of the programme is standardised to provide learners with a consistent learning experience, the diversity of teaching approaches and academic traditions represented within this European partnership is regarded as a strength. Accordingly, the standard module structure described above serves as a recommendation rather than a mandatory format.

In particular, learning materials, content input, and live sessions may be distributed across the full 12-week delivery period and are therefore not necessarily confined to the eight Lecture Weeks emphasized in the recommended standard structure.

Likewise, live sessions may be organised in different formats. For example, rather than offering eight weekly one-hour sessions, educators may combine contact hours into fewer but longer sessions, offer additional live learning opportunities, or adopt other pedagogically appropriate arrangements – provided that the programme's intended structure of predominantly flexible asynchronous learning, complemented by no less than eight hours of optional live interaction across the module, is maintained. Furthermore, detailed scheduling information must be provided transparently in the *Basic Course Information* prior to the start of the module.

Where appropriate, live sessions may also be shared across different Digital4Security learning offers, including degree programmes and microcredentials. Learners from different cohorts may therefore participate jointly in selected live activities.

While participation in live sessions is normally voluntary for learners enrolled in ASIIN-certified microcredentials, exceptions may apply where participation is required for specific assessment components, such as oral examinations or presentations. Such requirements shall be specified transparently in the relevant module information.

Learners are advised to consult the *Module Handbook* in combination with each module's *Basic Course Information* for further details, including the schedule and

any variations around the recommended standard structure described in Section 4.4.

4.7 Material Availability

Access to the digital learning materials is provided for the period required to complete the respective microcredential, in accordance with the D4S **General Terms and Conditions**.

For ASIIN-certified microcredentials, learners normally retain access to the online learning environment throughout the module delivery period, the assessment and grading process, and for a further **eight weeks following publication of the learner's final module grade**.

This additional access period is intended to allow learners to review the learning materials, feedback, and assessment results, and, where applicable, to exercise their rights under the complaints and appeals procedures set out in these *Study and Examination Regulations*.

Upon expiry of the access period, learners' access to the online learning environment and its digital learning materials may be withdrawn. This shall not affect the continued validity of any certificates, academic records, or other documentation previously issued by the Awarding Partner. Access to the learner's digital certificate will continue to be available through the Digital4Security infrastructure even after access to the module's learning materials has expired.

5. Modules

An overview of all modules that are available as ASIIN-certified microcredentials is provided in Table 3.

Table 3: Overview of Modules available as ASIIN-Certified Microcredentials

No.	Module Title	ECTS	Delivering Partner	Awarding Partner
1	Communication Design for Cybersecurity	5	UDS	UDS
2	Business Resilience, Incident Management and Threat Response	5	MTU	UDS
3	AI and Emerging Topics in Cybersecurity	5	UDS	UDS
4	Cybersecurity Culture, Strategy and Leadership	5	VMU/ ATAYA	UDS
5	Enterprise Architecture, Infrastructure Design and Cloud Computing	5	UPB/NCI	UDS
6	Law, Compliance, Governance, Policy and Ethics	5	UNIBS	UDS
7	Research Methods	5	UNI KO	UDS
8	Security Operations	5	CY CERGY	UDS
9	Technological Foundations in Computer Science and Security Controls	5	UPB	UDS
10	Automation of Security Tasks and Data Analytics	5	UNIRI	UDS
11	CISO and Crisis Communication	5	VMU/ ATAYA	UDS
12	Risk Management of Cyber-Physical Systems	5	POLIMI/ CEFRIEL	UDS
13	Cybersecurity Auditing	5	VMU/ ATAYA	UDS
14	Cybersecurity Economics and Supply Chain	5	MRU	UDS
15	Cybersecurity Education and Training Delivery I	5	BUT	UDS
16	Cybersecurity Education and Training Delivery II	5	UPB	UDS
17	Cybersecurity in Industry – Security of OT and Cyber-Physical Systems	5	POLIMI/ CEFRIEL	UDS
18	Cybersecurity Law and Data Sovereignty	5	BUT	UDS

No.	Module Title	ECTS	Delivering Partner	Awarding Partner
19	Machine and Deep Learning in Cybersecurity	5	UNIRI	UDS
20	Digital Forensics, Chain of Custody and eDiscovery	5	UPB/NCI	UDS
21	Threat Intelligence	5	UPB	UDS

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

- Module designation (name / title)
- Term(s) of delivery
- Delivering Partner
- Teaching methods
- Prerequisites for joining the module
- Module summary
- Module learning outcomes
- Weekly content overview
- Examinations and assessment formats
- Reading list

The language of instruction, credit value, approximate total learner workload, duration, qualification level, Awarding Partner and pass requirement are not included in the individual module descriptors, as they apply uniformly across all modules and are specified centrally in the *Module Handbook*.

The language of instruction is English. The credit value is 5 ECTS, corresponding to an approximate total learner workload of 125 hours across the 12-week term. All ASIIN-certified microcredentials are classified at EQF Level 7 (Master's level) and are awarded by UDS.

To pass a module, learners must achieve at least 60% of the total available points. The interpretation of performance levels is consistent across all modules and defined in Section 6 of the *Study and Examination Regulations*.

Workload is further organised as follows.

- Workload distribution: Approximately 10 hours of study per week over the 12-week term.
- Asynchronous and synchronous components: Learning takes place predominantly through asynchronous study, complemented by optional live interaction opportunities amounting to no less than eight hours across the term.
- Recommended standard structure: Live learning opportunities are typically organised as a regular Office Hour during each Lecture Week (eight one-hour sessions across the module). Additional activities, such as collaborative projects or laboratory work, may provide further opportunities for live interaction.
- Workload regulation: Details regarding the recommended standard structure and flexibility provisions are set out in Section 4 of the *Study and Examination Regulations*.
- Timetable: Module-specific arrangements are specified in each module's *Basic Course Information*.

The *Module Handbook* is accessible to all learners via the programme's learning platform and is regularly updated, subject to applicable legal, regulatory, accreditation, and quality assurance requirements. Core elements, such as the Intended Learning Outcomes, total module workload and ECTS credits may only be adjusted through formal re-accreditation. Other supporting details may be adapted to facilitate continuous improvement, provided they remain fully aligned with the fixed elements of the curricular framework.

6. Grading System

The grading framework is outlined in Table 4. It defines learner performance in relation to the module's Intended Learning Outcomes, based on the percentage of points achieved relative to the total points available.

The framework ensures consistency and transparency in evaluating academic achievement. It applies to all assessment components within a module, as well as to the overall evaluation of module performance.

Table 4: Grading Scheme

Points	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

7. Assessment, Proctoring, and Scalability

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

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

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

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

7.1 Awarding Partner Review

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

In cases where a module is delivered by an associate partner institution within the Digital4Security network, the design of the assessments is led by that institution. However, final grade assignment and quality assurance remain the responsibility of the Awarding Partner.

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

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

To ensure consistency across the programme, Delivering Partners must submit the following documentation to the Awarding Partner at least one month prior to the start of the teaching term:

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

The Awarding Partner or authorized representatives of D4S partner institutions evaluate the submitted materials to ensure alignment with applicable programme standards and regulations.

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

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

7.2 Assessment Transparency

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

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

7.3 Assessment Weighting and Proctoring Requirements

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

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

7.3.1 Proctored Assessment (≥60%)

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

Permitted forms of proctored assessment include:

- Online exams using a GDPR-compliant digital proctoring tool, such as SMOWL.
- Live oral presentations or defences conducted synchronously with identity verification.
- Hand-signed declarations of authorship confirming that the submitted work has been completed independently by the learner, that all sources and external contributions have been appropriately acknowledged, that any use of third-party or AI-supported tools has been appropriately disclosed, and that no unauthorised assistance has been received in the preparation of the submission.
- Employer- or work-verified projects, where an industry partner, supervisor, or professional mentor attests that the learner has completed the work independently (for further details on the procedure, see Section 7.8).

The programme shall ensure that all learners, regardless of employment status, have equitable opportunities to liaise with industry partners, supervisors, or professional mentors to complete the required assessments.

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

7.3.2 Continuous Assessment (≤40%)

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

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

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

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

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

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

- Feedback discussions in a live session,
- Written comments,
- Annotated submissions,
- Recorded voice or screen feedback,

- Peer input guided by clear rubrics,
- Instructor-prepared automated feedback, e.g., in the context of quizzes.

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

7.4 Resits and Repeat Assessments

Learning is a dynamic process, and occasional challenges are recognised as part of meaningful academic and professional development. To support learner success and uphold the integrity of the qualification, the programme provides clearly defined opportunities to re-sit examinations and repeat assessments. These measures are designed to enable learners to demonstrate mastery of the Intended Learning Outcomes, while maintaining fairness and upholding high academic standards across the programme.

7.4.1 Examination Opportunities per Module Enrolment

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

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

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

The dates or examination windows for both the Ordinary and Extraordinary Calls are published in advance and communicated to learners at the beginning of the term, as part of the *Basic Course Information*, and in accordance with the academic calendar requirements set out in Section 4.

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

7.4.2 Module Re-Enrolment

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

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

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

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

7.4.3 Maximum Number of Examination Attempts

No single examination may be attempted more than four times in total, including all attempts made across repeated module enrolments. Learners are strongly advised to monitor their number of attempts.

As the number of examination attempts is limited, all examination attempts are recorded as part of the learner's academic record. An examination attempt is deemed to commence with the learner's first assessment-relevant submission, which will typically occur in Lecture Week 1 (corresponding to Week 3 of the 12-week term). Up to that point, learners may withdraw from the module without an examination attempt being recorded. Once the first assessment-relevant submission has been made, however, the examination attempt counts in full, even if the learner subsequently withdraws from the module, submits no further coursework, or does not attend the final examination. Consequently, learners enrolled in microcredentials should be aware that the same module cannot be attempted an unlimited number of times.

7.5 Late Submission of Coursework

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

7.5.1 Exceptional Circumstances

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

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

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

7.5.2 Procedure for Requesting Late Submission

Learners shall take the following steps when seeking an extension due to exceptional circumstances:

- **For a single module**: Contact the main course instructor from the Delivering Partner institution. With valid documentation, the instructor may grant a short extension or propose an alternative assessment arrangement at their discretion.
- **For multiple modules**: If the issue affects the learner's ability to engage with several modules (e.g., due to a natural catastrophe or medical emergency), the learner shall contact **coordinator.uds@digital4security.eu**, copying all main instructors from Delivering Partner institutions in the communication.
- **For general academic challenges**: If the learner is falling behind more broadly (e.g., across multiple modules, due to time management issues or personal circumstances), they should contact **studyaffairs@digital4security.eu**. The team can assist in identifying suitable support measures.

7.5.3 Unacceptable Grounds for Late Submission

The following are not considered valid grounds for late submission:

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

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

7.6 Scalable Assessment Formats

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

Two approaches are especially recommended:

- Team-Based Assignments
- Peer Assessment

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

Further recommendations for online assessment can be found in the *Practical Guide for Lecturers*, and in the Scientific Report *Assessment Methods for Online Teaching* by UDS.

7.7 Appealing Assessment Outcomes

7.7.1 Grading Appeals

Learners wishing to contest a grade should first submit an **informal request** for an **assessment review session with the responsible examiner** within one week of the grade being issued. The review session should then take place within one week of the learner's request. This session provides an opportunity for learners to discuss the evaluation and seek clarification. The examiner may convene a joint review session for all learners in the module and is not obliged to accommodate

individual scheduling requests, though individual meetings may be offered at the examiner's discretion.

If concerns remain unresolved after the review session, learners may submit a formal grade appeal within three weeks from the issuance of the original grade. Appeals shall first be addressed to the **Delivering Partner**.

Should the matter remain unresolved within two weeks following the submission of a formal grade appeal, it may be brought to the attention of the **Programme Coordinator** at the Awarding Partner institution, by sending an email to **coordinator.uds@digital4security.eu**. A reasoned outcome should ordinarily be communicated within a further two weeks.

Should the matter remain unresolved at this stage, the appeal may be escalated to the Awarding Partner's **Examinations Board**, which can be contacted by email to **examinations@digital4security.eu**. The Board shall provide a reasoned decision within four weeks of receiving the appeal.

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

7.7.2 Peer Review Appeals

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

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

learner may then request an informal grade review session with the instructor within one week of this date, following the procedure outlined in Section 7.7.1

7.8 Workplace Attestation

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

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

The attestation must be signed by a person with direct supervisory or oversight responsibility, who is not subordinate to the learner and free from conflicts of interest - for example, not a business partner, close personal associate, or someone under the learner's authority (e.g., not an organization's employee if the learner is the organization's CEO).

Eligible individuals include:

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

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

8. Academic Integrity, and Support for Good Scholarly Practice

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

Academic misconduct

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

General misconduct

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

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

8.1 Fostering Integrity and Empowering Learners as Ethical Professionals

Academic integrity is a cornerstone of scholarly and professional life. In this programme, integrity is not enforced through suspicion, but cultivated through clarity, support, and shared purpose. It is trusted that learners given the appropriate

tools, expectations, and respect will rise to excellence in both method and mind-set.

8.1.1 Learning to Use Artificial Intelligence (AI) Tools Responsibly

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

Instructors may define, for each assignment:

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

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

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

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

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

8.1.2 Building Confidence in Original Work

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

This includes learning to:

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

To support this:

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

8.1.3 Collaborative Learning vs. Collusion: Clarifying Expectations

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

Guidelines:

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

8.2 Responsible Use of Digital Platforms and Resources

The ASIIN-certified microcredentials provide access to a range of digital platforms, communication tools, and learning resources essential for teaching, collaboration, and assessment. These may include the Learning Management System, video-conferencing facilities, digital libraries, and other network-based services maintained by the partner institutions. The responsible and lawful use of these resources is integral to maintaining academic integrity, safeguarding personal data, and fostering a constructive learning environment.

8.2.1 Digital Etiquette (Netiquette)

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

8.2.2 Confidentiality of Assessment Materials and Individual Answers

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

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

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

The following exceptions apply:

- In team-based projects, assigned team members are expected to share relevant materials among themselves to collaboratively fulfil their joint tasks.
- In work-based projects, learners may discuss their work with mentors, supervisors, and colleagues, provided that any assistance received complies

with the applicable assessment requirements, is appropriately acknowledged where required, and does not compromise the learner's independent authorship of the submitted work.

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

8.2.3 Use of Learning Materials

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

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

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

8.2.4 System Security

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

8.3 Handling Suspected Misconduct: A Transparent and Supportive Process

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

Process Overview:

- Whether a concern exists shall ordinarily be determined by the Delivering Partner, in alignment with the Programme Coordinator at the Awarding Partner institution, who shall be contacted by email at **coordinator.uds@digital4security.eu** without undue delay after the matter has come to the Delivering Partner's attention. Where both parties are in agreement, the learner shall be formally notified of the concern. In exceptional circumstances, a concern may also be raised by other parties, for example as part of programme quality assurance activities.
- The learner shall receive formal notification of the concern without undue delay. This notification will ordinarily be sent by the Delivering Partner, with **coordinator.uds@digital4security.eu** copied on the correspondence. Should the Delivering Partner be unavailable, the notification may instead

be issued by the Programme Coordinator. The learner shall be offered the opportunity to respond within two weeks of notification.

- Based on the original concern and any response received from the learner within the two-week response period, the Examinations Board shall conduct a review within four weeks of notification.
- For complex cases, the Examinations Board may convene a Disciplinary Committee, including faculty from the Awarding Partner and the Digital4Security network. The Committee shall provide a final judgement within a further four weeks.
- Sanctions shall be proportionate, and developmental whenever possible:

    - Constructive feedback or revised submission.
    - Grade adjustment or nullification.
    - Temporary suspension or, in the most serious or repeated cases, expulsion from the programme.

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

Learners may appeal any disciplinary decision in writing within 14 calendar days of formal notification. The appeal must clearly state the grounds for appeal and be submitted via email to **examinations@digital4security.eu**, copying **secretariat@digital4security.eu** and **coordinator.uds@digital4security.eu** on the correspondence.

A formal response to the appeal shall be issued to the learner by the Examinations Board as early as reasonably practicable and, during any active term (excluding the Summer Period), no later than four weeks after the appeal has been received by the Board.

8.4 European and National Codes of Conduct

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

8.5 Mutual Trust and Shared Responsibility

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

As a programme, we commit to:

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

Learners are encouraged to:

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

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

9. Microcredential Completion and Certification

9.1 Award Criteria

To be eligible for the award of the microcredential certificate, a learner must:

- Be formally admitted to the learning offer;
- Pass the learning offer by achieving at least 60% of the available total points;
- Comply with any additional requirements outlined in the programme regulations, such as adherence to academic integrity standards.

9.2 Certification upon Successful Completion

Upon successful completion of a microcredential, learners receive an official **Microcredential Certificate** issued by the German University of Digital Science (UDS). The certificate confirms that the learner has successfully achieved the Intended Learning Outcomes of the respective module and fulfilled all applicable academic and assessment requirements in accordance with these *Study and Examination Regulations*. The certificate is issued in digital form and incorporates appropriate measures to support authenticity and verification.

To facilitate transparent academic and professional recognition, the certificate provides comprehensive information about the completed learning offer. Depending on the specific module, the certificate includes, where applicable:

- the learner's name;
- the title of the completed microcredential (module);
- the issuing institution and, where applicable, the delivering institution(s);
- the term in which the module was completed;
- the mode of delivery (online);
- the workload in hours (approximately 125);
- the awarded ECTS credits (5 ECTS);

- the qualification level within the European Qualifications Framework (EQF level 7);
- the principal subject areas;
- the language of instruction (English);
- any applicable module prerequisites;
- the Intended Learning Outcomes achieved;
- the assessment method(s);
- information on supervision or identity verification;
- the final result achieved, including the point value and grade or performance level;
- information regarding the applicable quality assurance and external certification;
- information supporting the academic recognition of the microcredential;
- the certificate identification number and verification mechanism; and
- the date of issue.

The exact content and format of the certificate may be updated over time in response to evolving national, European, or international recommendations regarding the documentation of microcredentials, provided that such changes do not affect learners' academic rights or the substantive information certified.

10. Context of the ASIIN-Certified Microcredentials

10.1 Planned Online Master's Programme

The ASIIN-certified microcredentials form part of a planned **60 ECTS Online Master's Degree Programme in Cybersecurity Management and Data Sovereignty**. Beyond the general Master's degree award, this programme is designed to support tailored career preparation by enabling participants to specialise in one of six **ENISA professional profiles**.

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

While the Online Master's programme is not yet available for enrolment, pending completion of the applicable national accreditation procedures, it is planned to comprise the following structure:

- **30 ECTS – Compulsory Components:**
  - *15 ECTS* in mandatory taught modules
    - Communication Design for Cybersecurity
    - Business Resilience, Incident Management and Threat Response
    - Ethical Hacking and Penetration Testing

- *15 ECTS* allocated to the Master's thesis (which, if a professional profile has been selected, is aligned with that area of specialisation)

- **30 ECTS – Elective Components:**
  - *20 ECTS* in elective modules aligned with a selected professional profile (with up to six recommended modules available per profile), supporting optional career specialisation
  - *10 ECTS* in freely chosen elective modules, allowing for individual academic and professional development

Selection of a professional profile is recommended, but not mandatory. Learners may alternatively complete all **30 ECTS** of elective study through freely chosen modules.

Beyond the **21 modules** currently available as ASIIN-certified microcredentials, three additional modules are planned to form part of the Online Master's programme. These comprise the *Master's Thesis* and two modules designed and delivered by the Spanish partner UNIR. The latter were not included in the ASIIN certification procedure, because the applicable institutional and Spanish national frameworks governing the respective microcredentials were still evolving at the time of the certification review. They comprise the planned modules *Ethical Hacking and Penetration Testing* as well as *Malware Analysis*.

10.2 Progression towards the Online Master's Programme

Within the planned framework, it is expected that learners will be able to obtain recognition for at least one previously completed microcredential, thereby reducing the remaining study workload accordingly. In this case, the remaining workload to be completed within the Master's programme would be reduced to 55 ECTS. Whether recognition may also be granted for additional microcredentials – up to a maximum of 50% of the overall programme workload – is currently under exploration and cannot be guaranteed at this stage.

10.3 Admission Context of the Planned Master's Programme

Unlike the microcredentials governed by these *Study and Examination Regulations*, admission to the planned Online Master's programme will be subject to formal educational eligibility requirements. These are expected to include a Bachelor's degree in any discipline and prior learning corresponding to at least 240 ECTS. The latter may be demonstrated through a Bachelor's degree, previously completed microcredentials (with all D4S microcredentials automatically recognized), relevant professional experience, or other recognised forms of prior learning, subject to the applicable admission and recognition regulations.

10.4 Programme Learning Outcomes

The planned Online Master's programme is designed to convey the Programme Learning Outcomes (PLOs) presented in Table 5.

Table 5: Overarching Learning Goals across the Planned Online Master's Programme

No.	Programme Learning Outcomes
PLO1	Critically assess and evaluate cybersecurity principles, practices, and technologies relevant to modern enterprises.
PLO2	Strategically apply cybersecurity knowledge and utilise practical skills and technologies for long-term success in cybersecurity leadership roles across diverse industries, government agencies, and institutional settings.
PLO3	Identify knowledge gaps and undertake self-learning to acquire new knowledge to support professional development and the ability to adapt to evolving threats, technologies, and regulatory environments.
PLO4	Exhibit and apply leadership skills necessary for effectively managing cybersecurity initiatives within organisations, including education and training, strategic planning, and resource allocation.
PLO5	Critically evaluate and analyse cyber threats in order to implement effective security operations, and to enable the proactive identification, assessment, and mitigation of cyber threats.
PLO6	Effectively apply analytical and strategic thinking in order to make decisions to address security requirements.

PLO7	Communicate effectively across a range of complex and advanced cybersecurity concepts to provide leadership within an organisation and facilitate effective collaboration and teamwork.
PLO8	Critically assess cybersecurity legal, information governance, and regulatory frameworks and practices to ensure effective oversight, auditing, risk mitigation, accountability, compliance, and strategic alignment with organisational objectives.

The curriculum modules are mapped to the Programme Learning Outcomes (PLOs) as outlined in Table 6. Both the module content and the associated assessments are designed to effectively support the PLOs to which the respective module is assigned.

Table 6: Overview of Each Module's Contribution to the Programme's Learning Outcomes

No.	Module	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8
1	*Communication Design for Cybersecurity*	X	X	X	X		X	X	X
2	*Business Resilience, Incident Management and Threat Response*	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		

No.	Module	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8
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

10.5 Current EU Project Funding

Learners currently benefit from the circumstance that ASIIN-certified microcredentials are offered within the framework of the EU-funded Digital4Security project. Through 50% co-funding provided by the European Union, participation fees are reduced to half of the standard tuition fee. This funding arrangement applies until the end of the project on 30 September 2027. Until then, learners have the opportunity to access high-quality, externally quality-assured university education at substantially reduced cost.

Following the end of the EU co-funding period, participation fees for newly purchased microcredentials are expected to revert to the standard tuition fee applicable at that time. Learners wishing to benefit from the reduced project-funded fees are therefore encouraged to take advantage of this opportunity while it remains available.

Document Governance

These *Study and Examination Regulations* apply in conjunction with the associated *Module Handbook*, the applicable *Product Information*, and the Digital4Security *General Terms and Conditions*. The Awarding Partner is responsible for the content and maintenance of these *Study and Examination Regulations*.

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

1. Study and Examination Regulations
2. Module Handbook
3. Digital4Security **General Terms and Conditions**
4. Other supporting documentation, including Product Information published on the Digital4Security website at **www.digital4security.eu**

Correspondence regarding proposed refinements in these *Study and Examination Regulations* shall be addressed to **secretariat@digital4security.eu**, with **coordinator.uds@digital4security.eu** copied on the correspondence. The Secretariat also supports the monitoring of all programme documents to ensure that any substantive changes, i.e. those not of an editorial nature, are duly reflected across all affected documents.

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

Amendments shall not apply retroactively to academic cohorts already enrolled in the programme, unless it can be reasonably assumed that the amendment is in

the learners' interest or will not result in any detriment to their academic standing. In particular, no amendment shall adversely affect:

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

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

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

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