



**Digital4Security**

Shaping Europe's cyber future

# Digital4Security Launch Campaign & Student recruitment

Deliverable 5.3

## Table of Contents

<b>Executive summary.....</b>	<b>3</b>
D5.3 Digital4Security Launch Campaign & Student Recruitment.....	3
Key Campaign Goals: .....	3
Expected outcomes: .....	3
The Digital4Security Consortium .....	4
Document control information .....	6
<b>Introduction .....</b>	<b>7</b>
Purpose of the launch campaign .....	7
Objectives of student recruitment.....	7
<b>Target audiences and messaging.....</b>	<b>8</b>
Target audiences.....	8
Key messaging and value proposition.....	8
<b>Launch campaign components .....</b>	<b>9</b>
Overview of campaign components & assets.....	9
Branding and visual identity guidelines .....	10
Digital Assets & Website.....	14
Prospectus and flyers:.....	14
Dedicated pages on the Website:.....	14
Modules landing pages:.....	14
Digital Marketing Activities .....	17
Social media strategy – Partner channels and project LinkedIn page .....	17
Email marketing.....	17
Webinars and live events.....	19
Partnerships and collaborations.....	19
Digital Skills and Jobs Platform.....	19
<b>LinkedIn campaign and content strategy.....</b>	<b>21</b>
Digital4Security LinkedIn content strategy.....	21
Content types and posting schedule (subject to revision) .....	21
Suggested messaging .....	22

Visual and branding guidelines .....	22
Calls to action.....	22
Sample creatives and assets.....	22
Sample creatives for campaigns .....	23
Canva assets .....	27
Partner activation packs for the Digital4Security launch campaign.....	30
Sample content calendar .....	31
<b>Recruitment and onboarding.....</b>	<b>34</b>
Enrollment goals and targets .....	34
Recruitment Channels .....	34
Engagement with high schools, universities, and industry associations.....	35
Full Fabric admission and enrolment.....	36
Embedded Full Fabric forms on project website.....	36
Emails.....	43
<b>Timeline and milestones .....</b>	<b>47</b>
Key phases of the campaign .....	47
<b>Milestones for tracking progress .....</b>	<b>48</b>
<b>Monitoring and evaluation .....</b>	<b>50</b>
Metrics and KPIs to measure success .....	50
Tools and methods for data collection and analysis.....	50
Feedback mechanisms and continuous improvement.....	51
<b>Risks and mitigation strategies.....</b>	<b>52</b>
Potential challenges and obstacles.....	52
Contingency plans .....	52
<b>GDPR .....</b>	<b>53</b>

## Executive summary



### D5.3 Digital4Security Launch Campaign & Student Recruitment

Digital4Security is a ground-breaking pan-European master's programme aimed at addressing the escalating challenges posed by cybersecurity threats and data privacy concerns across all industries. With funding of almost €10 million from the European Union, this four-year initiative is led by a Consortium of 34 partners spanning 14 countries. This industry-driven programme will provide comprehensive knowledge of cybersecurity management, regulatory compliance, and technical expertise to European SMEs and companies.

Deliverable D5.3 – Digital4Security Launch Campaign & Student Recruitment v1 outlines a strategic approach designed to effectively launch and promote the Digital4Security Masters Programme, aiming to recruit a diverse and talented group of students. This document serves as a comprehensive guide to the initial campaign and ongoing recruitment efforts, aligning closely with the project's overarching goals of enhancing cybersecurity skills across Europe.

#### Key Campaign Goals:

- Establish and promote the Digital4Security brand.
- Attract, engage, and enrol students from varied backgrounds, with an emphasis on inclusion and diversity.
- Strengthen ties with industry partners and educational institutions to enhance the programme's reach and impact.

#### Expected outcomes:

- Successful launch of the Digital4Security Master's Programme.
- Achievement of enrolment targets for the first cohort.
- Establishment of a sustainable recruitment strategy that can be adapted for future cycles.

## The Digital4Security Consortium

The Digital4Security Consortium is a dynamic pan-European partnership of innovators in the field of cybersecurity. It comprises higher education institutions, industry partners, training providers and cybersecurity clusters, working together to design, promote and deliver a transformative cybersecurity management programme, developed and delivered by the best cybersecurity talent from Europe and worldwide.

No.	Role	Short name	Partner	Country
1	COO	POLITEHNICA BUCHAREST	NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY POLITEHNICA BUCHAREST	RO
2	BEN	SA	SCHUMAN ASSOCIATES SCRL	BE
3	BEN	Ataya	ATAYA & PARTNERS	BE
4	BEN	POLIMI	POLITECNICO DI MILANO	IT
5	BEN	CMIP	POLSKI KLASTER CYBERBEZPIECZENSTWA CYBERMADEINPOLA ND SP. Z O. O.	PL
6	BEN	Contrader	CONTRADER SRL	IT
7	BEN	DTSL	DIGITAL TECHNOLOGY SKILLS LIMITED	IE
8	BEN	indiepics	INDEPENDENT PICTURES LIMITED	IE
9	BEN	MATRIX	MATRIX INTERNET APPLICATIONS LIMITED	IE
10	BEN	PROFIL KLETT	PROFIL KLETT D.O.O.	HR
11	BEN	ServiceNow	SERVICENOW IRELAND LIMITED	IE
12	BEN	UNIBS	UNIVERSITA DEGLI STUDI DI BRESCIA	IT
13	BEN	UDS	UNIVERSITY OF DIGITAL SCIENCE GGMBH	DE
14	BEN	SKILLNET	SKILLNET IRELAND COMPANY LIMITED BY GUARANTEE	IE
15	BEN	IT@CORK	IT@CORK ASSOCIATION LIMITED LBG	IE
16	BEN	ADECCO TRAINING	ADECCO FORMAZIONE SRL	IT
17	BEN	UNI KO	UNIVERSITAT KOBLENZ	DE
18	BEN	BRNO UNIVERSITY	VYSOKE UCENI TECHNICKE V BRNE	CZ
19	BEN	MTU	MUNSTER TECHNOLOGICAL UNIVERSITY	IE
20	BEN	DIGITAL SME	EUROPEAN DIGITAL SME ALLIANCE	BE
21	BEN	DIGITALEUROPE	DIGITALEUROPE AISBL*	BE
22	BEN	MRU	MYKOLO ROMERIO UNIVERSITETAS	LT
23	BEN	UNIRI	SVEUCILISTE U RIJECI	HR

24	BEN	NASK	NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTU T BADAWCZY	PL
25	BEN	UNIR	UNIVERSIDAD INTERNACIONAL DE LA RIOJA SA	ES
26	BEN	NCI	NATIONAL COLLEGE OF IRELAND	IE
27	BEN	TERAWE	TERAWE TECHNOLOGIES LIMITED	IE
28	BEN	CY CERGY PA RIS	CY CERGY PARIS UNIVERSITE	FR
29	BEN	BANCO SANT ANDER	BANCO SANTANDER SA	ES
30	BEN	CYBER RANGE S	CYBER RANGES LTD	CY
31	BEN	RED OPEN S. R.L.	RED OPEN S.R.L.	IT
32	BEN	VMU	VYTAUTO DIDZIOJO UNIVERSITETAS	LT
33	AP	FHG	FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV	DE
34	AP	Pearson Benelux	Pearson Benelux BV	NL

## Document control information

Project	Digital4Security
<b>Document title</b>	D5.3 Digital4Security Launch Campaign & Student recruitment v1
<b>Work Package number</b>	WP5
<b>Deliverable number</b>	D5.3
<b>Lead beneficiary</b>	Matrix Internet
<b>Project coordinator:</b>	National University of Science and Technology POLITEHNICA Bucharest (NUSTPB)
<b>Dissemination level</b>	PU - Public
<b>Authors</b>	Aoife O'Driscoll, Fionnuala Mahon, Matrix Internet, Diarmaid Mac Mathúna, Indiepics
<b>Reviewers</b>	Irene Marinelli, DIGITALEUROPE (1st level review) Kinga Iwan, Karolina Wojtyczek CMIP (2nd level review) POLITEHNICA Bucharest (final review)
<b>Description</b>	Set up the Digital Learning Platform and Teaching Tools for the online masters programme
<b>Status</b>	Final
<b>Delivery date</b>	09.11.2024
<b>Due date</b>	30.11.2024
<b>Approval date:</b>	30.11.2024

## Revision history

Version	Date	Modified by	Comments
1	02.11.2023	Aoife O'Driscoll, Fionnuala Mahon, Matrix Internet	Draft for QA review
1	09.11.2023	Irene Marinelli, DIGITALEUROPE	1st level review
2	23.11.2023	Kinga Iwan, Karolina Wojtyczek CMIP, Brian Cochrane, Schuman Associates	QA reviewers
3	30.11.2023	Florin Pop, Politehnica Bucharest	Final review
4	30.11.2023	Giuseppe Ditaranto, Fionnuala Mahon, Matrix Internet	Final review and layout

## Introduction



### Purpose of the launch campaign

The launch campaign for Digital4Security aims to introduce and establish the Digital4Security Masters Programme as a leading educational initiative in Cybersecurity Management & Data Sovereignty across Europe. The campaign is designed to generate awareness, interest, and engagement among potential students and partners, showcasing the unique benefits and opportunities offered by the programme. The strategic promotion will leverage both digital and traditional media to reach a broad audience, ensuring high visibility and impact at a pan-European level.

### Objectives of student recruitment

The primary objectives of the student recruitment strategy for Digital4Security include:

- **Attracting a diverse student body:** Targeting a wide range of applicants, including professionals in cybersecurity, non-ICT professionals looking to transition into cybersecurity roles, and recent graduates seeking specialised knowledge in cybersecurity management.
- **Ensuring high-quality enrolment:** Focusing on attracting qualified candidates who can contribute to and benefit from the programme, thereby enhancing the learning experience for all participants.
- **Promoting inclusivity and accessibility:** Making the programme accessible to a diverse audience, including underrepresented groups in the field of cybersecurity, to foster a more inclusive cybersecurity workforce.



## Target audiences and messaging



### Target audiences

The Digital4Security launch campaign targets a diverse group of potential students and institutional partners across Europe. These include:

- **Cybersecurity professionals and practitioners** seeking to enhance their expertise and credentials.
- **Non-ICT professionals** interested in transitioning to cybersecurity roles.
- **Academic institutions and training providers** who can integrate the Digital4Security curriculum into their offerings.
- **Businesses and SMEs** requiring advanced cybersecurity training for their staff.
- The campaign also aims to engage **policymakers and educational influencers** to advocate for the integration of the programme into broader educational and professional training frameworks.

### Key messaging and value proposition

The key messaging of the Digital4Security launch campaign will focus on the critical importance of advanced cybersecurity training and the unique benefits of the programme, such as:

- **Comprehensive education:** Offering a complete suite of modules that address both the managerial and technical aspects of cybersecurity.
- **Expert-led training:** Learning from leading cybersecurity experts from across Europe.
- **Career advancement:** Enhancing career prospects in a high-demand field.
- **Network building:** Connecting with other cybersecurity professionals and industry leaders.

## Launch campaign components



### Overview of campaign components & assets

The Digital4Security launch campaign is designed to maximize outreach and engagement with potential students and partners:

- **The Digital4Security brand** - The campaign will launch the new brand into the market, positioning D4S as a highly innovative and market leading cybersecurity masters.
- **The project website** will inform prospective students about the course, giving an overview of the programme, including modules, application details, and the flexibility of online learning. Highlighting which modules are mandatory and the elective options, Full Fabric student enrolment platform, the Moodle LMS, a dedicated project newsletter, and a robust presence on social media platforms.
- **Students focused master's landing page** - An overview of the programme, including modules, application details, and the flexibility of online learning.
- **Prospectus:** A guide to the programme, featuring a welcome note from the Course Coordinator, detailed module descriptions, and partner profiles.
- **Brochures:** Flyers for each module, with detailed descriptions of content and benefits.
- **Student Handbook:** A comprehensive look at student life and available services.
- **Module summary flyer:** A quick visual guide to all modules, perfect for sharing.
- **Social Media Strategy:** Content marketing via LinkedIn and partner social media channels.
- **Email marketing:** Outreach via the projects email newsletter, direct outreach to stakeholders and promotion via the partner's email channels.

- **Digital Skills and Jobs Platform:** Community engagement, direct communication and promotion on DSJP Training Opportunities page.
- **Webinars and live events:** Promotional webinars to launch the programme and participation in both online and face to face events targeted at SMEs.

## Branding and visual identity guidelines

The branding strategy for Digital4Security ensures that all communication materials reflect the core values and professionalism of the programme. The visual identity includes:

**Logo usage:** Guidelines on how to use the Digital4Security logo across various media. We have included a few images from the branding guidelines for illustrative but the deliverable 5.1 includes the brand guidelines viewable [here](#) and were distributed to all partners and are accessible on the project SharePoint.

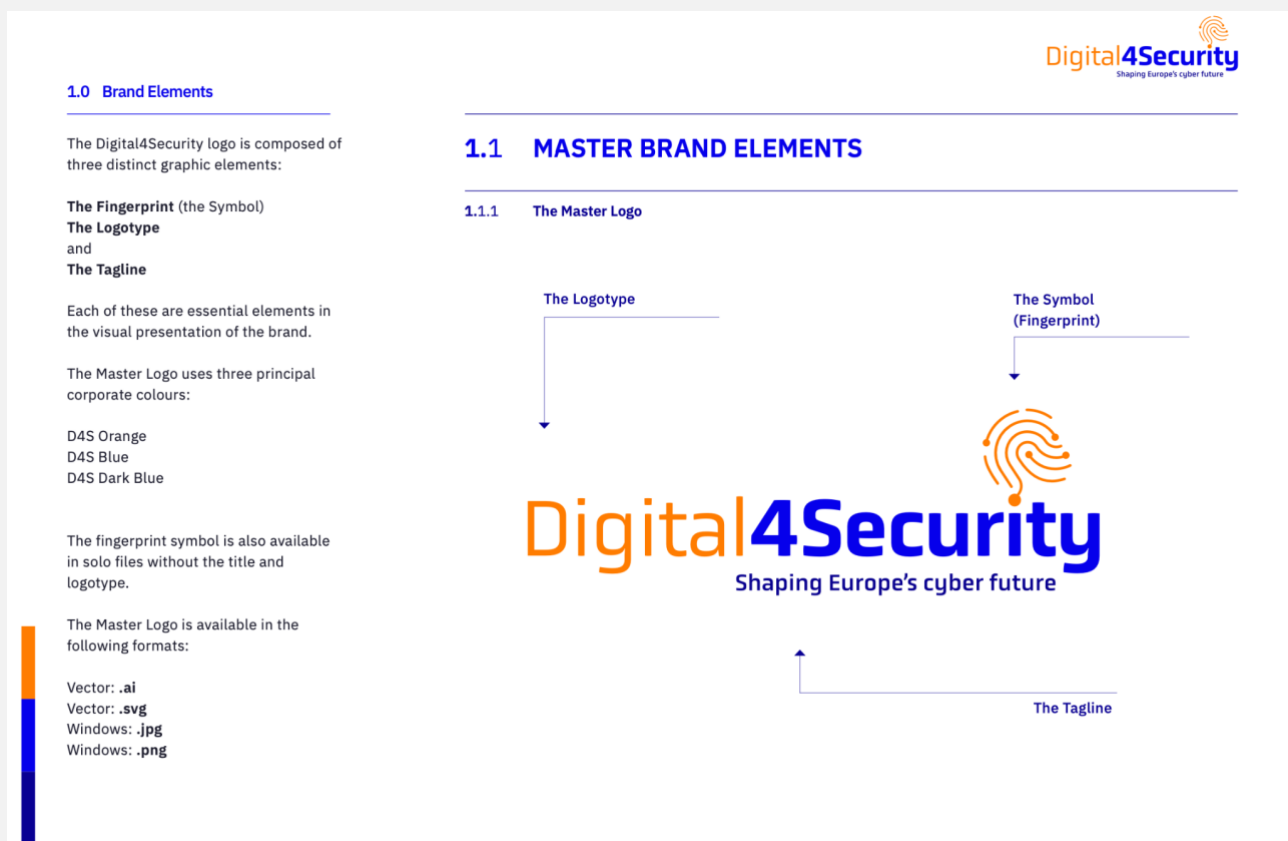


Figure 1: Master Brand elements - the Master Logo

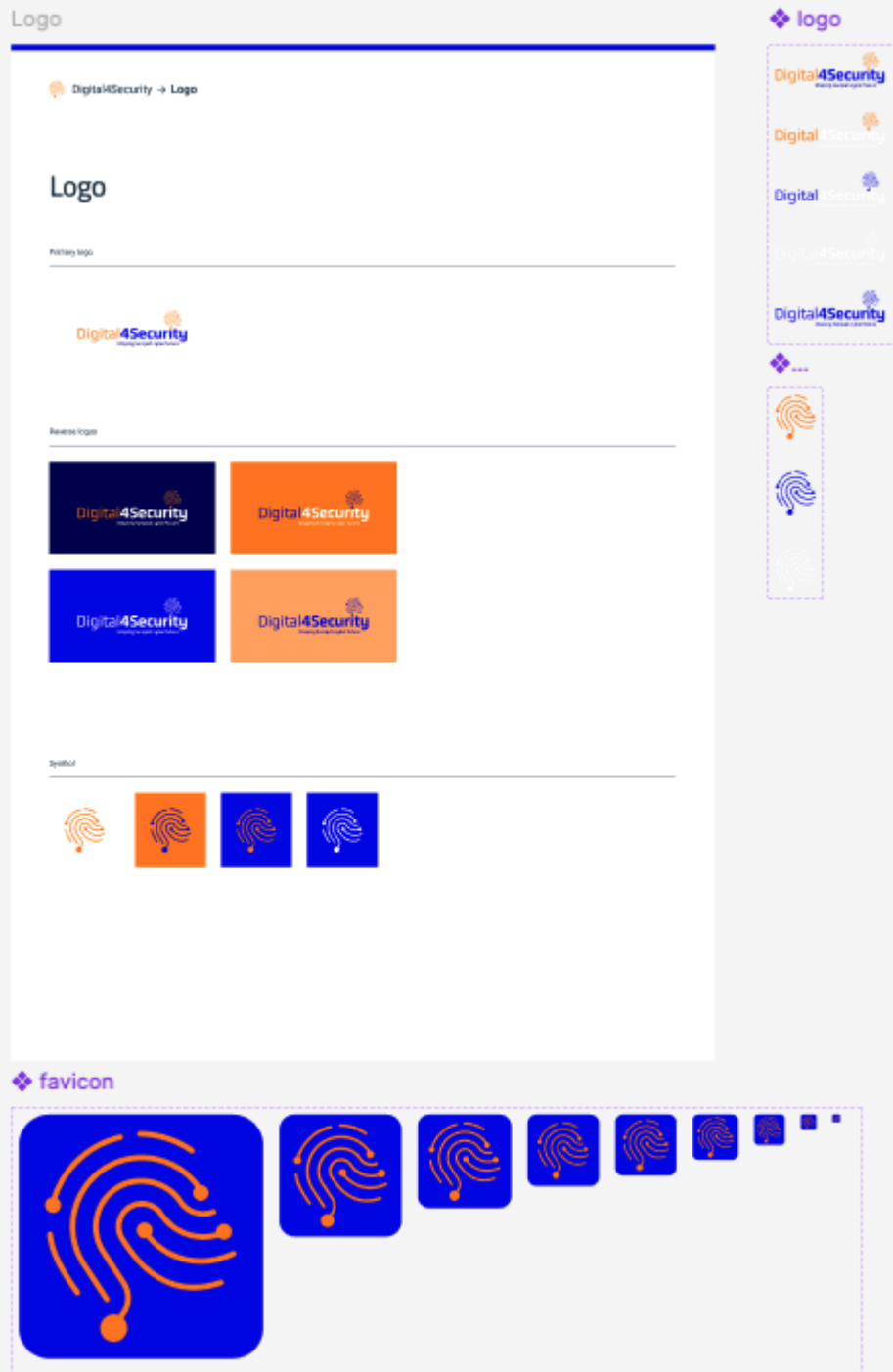


Figure 2: Digital4Security design system logo assets

**Colour palette:** A specific set of colours that align with the themes of security, trust, and technology.

Digital4Security → Colours

## Colours

Our design system leverages a purposeful set of color styles as the perfect starting point for any brand or project. When it comes to color, contrast is critical for ensuring text is legible. We've added WCAG 2.1 contrast ratios to our color system so you can make sure you're designing with accessibility in mind.

### Primary colours

These are the main colors that make up the majority of the colors used in the design system.

**Primary D4S Orange**  
The primary color is your "brand" color, and is used across all interactive elements such as buttons, links, inputs, etc. This color can define the overall feel and can elicit emotion.

2.58	AAA 9.72
500 #FF7C00	300 #FFA861

**Primary Blue**

AAA 16	AAA 9.51	AAA 14.66	AAA 18.51
200 #DEDEFF	500 #0600EB	600 #090093	700 #000056

**Gradient**

AAA 9.51
Gradient

**Base**

AAA 21:1
White #FFFFFF

**D4S Slate**

AAA 19.55	AA 11.11	AA 5.27	AAA 13.29	AAA 16.87	AAA 18.94	AAA 19.79
500 #07072B	400 #393955	300 #6A6A80	200 #CDCDD5	100 #E6E6EA	50 #F3F3F4	10 #F8F8F9

---

### Secondary colours

Along with primary colors, it's helpful to have a selection of secondary colors to use in components such as pills, alerts and labels. These secondary colors should be used sparingly or as accents, while the primary colors should take precedence.

**Light blue**

AAA 16
500 #DEDEFF

**Yellow**

AAA 12.1
500 #FFB800

Figure 3: Digital4Security project brand colours.

**Typography:** Standardised fonts that ensure clarity and consistency across all communications.

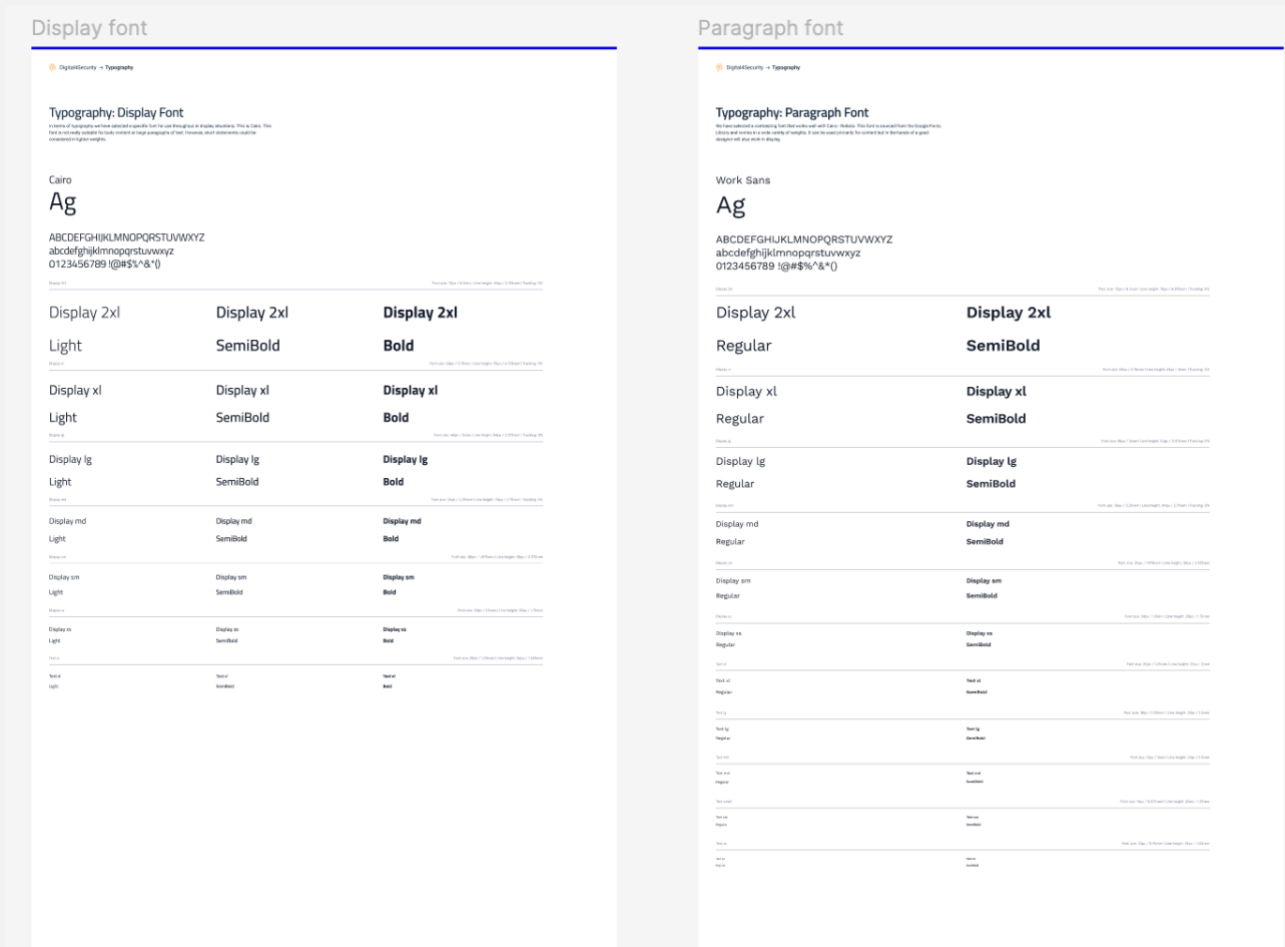


Figure 4: Digital4Security project typography.

- **Imagery and graphics:** High-quality images and graphics that resonate with the target audiences and reinforce the campaign's key messages.

These elements are designed to create a cohesive and recognisable brand identity that communicates the reliability, sophistication, and importance of the Digital4Security programme.

## Digital Assets & Website

### Prospectus and flyers:

- **Purpose:** Serve as comprehensive guides to the Digital4Security programme, featuring a welcome note from the Course Coordinator, detailed module descriptions, and partner profiles.
- **Distribution:** promoted to download at industry conferences, educational fairs, and can be requested via the website.

### Dedicated pages on the Website:

- **Content:** The masters has a dedicated, student-focused page on the project website: <https://www.digital4security.eu/student-landing-page/> which will be continually updated. Informing prospective students about the course, giving an overview of the programme, including modules, application details, and the flexibility of online learning. Highlighting which modules are mandatory and the elective options. Each module will also have a dedicated page and as the content becomes available we'll update each module, featuring introduction videos that outlines the module's objectives, key takeaways, and instructor insights. <https://www.digital4security.eu/module/ai-and-emerging-topics-in-cybersecurity/> is an example and we have a landing page for each module and will update as more information becomes available.
- **Interactive elements:** Prospective students can download master prospectus, student handbook, engage with FAQs directly via the project website and be guided to the online application form or register their interest in future enrolment opportunities.

### Modules landing pages:

Each module has its own landing page and this will be updated as new content is made available and the module descriptions were rewritten from the Student Handbook to be for the targeted audience. We've a template ready with the following key elements

- Module description.
- Module highlights with call to action to register interest or apply for course.
- Full course breakdown and subjects covered
- Introduction video
- Module leader(s)
- Related FAQs

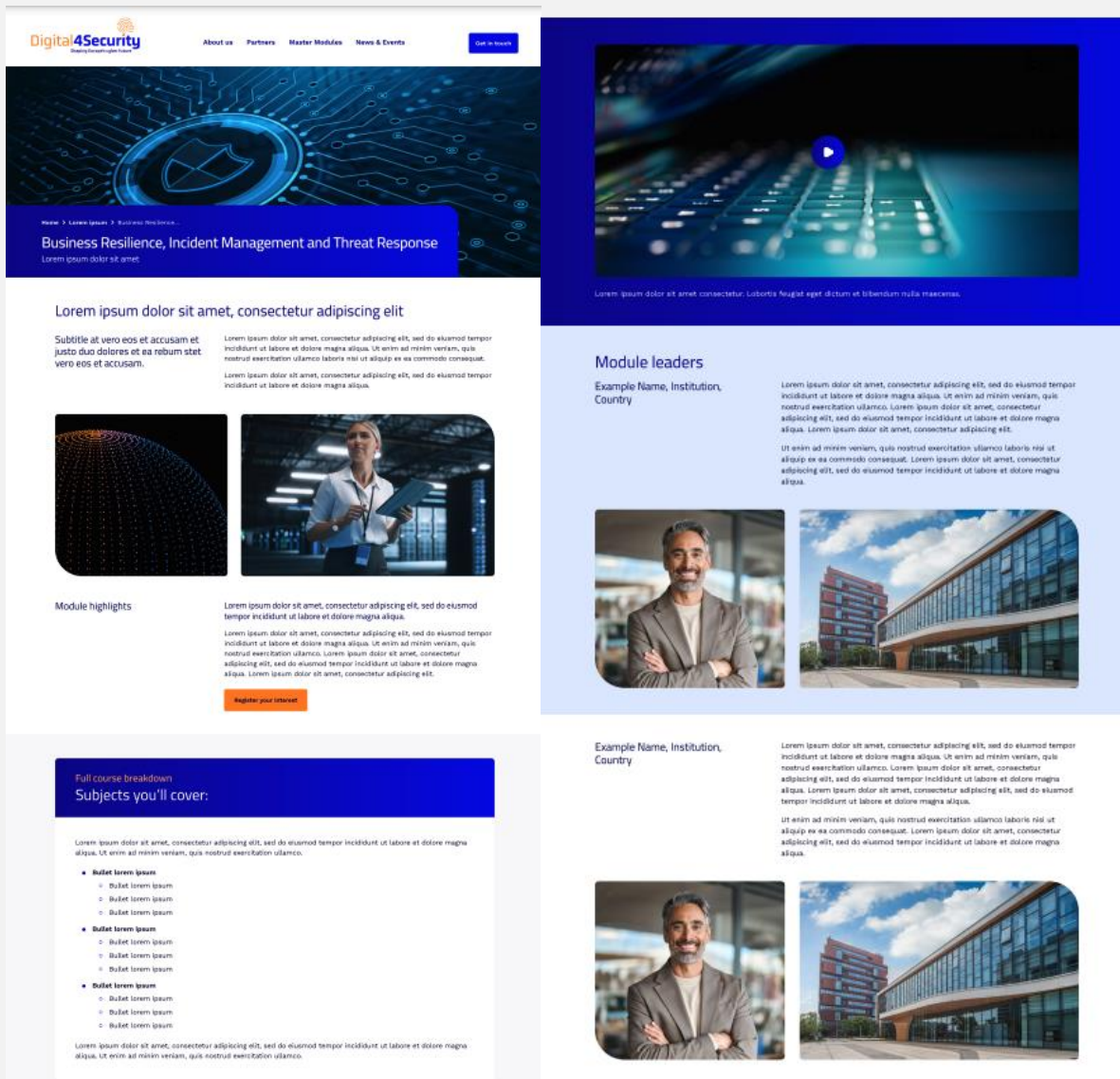


Figure 5: mock-up of design for Module landing page



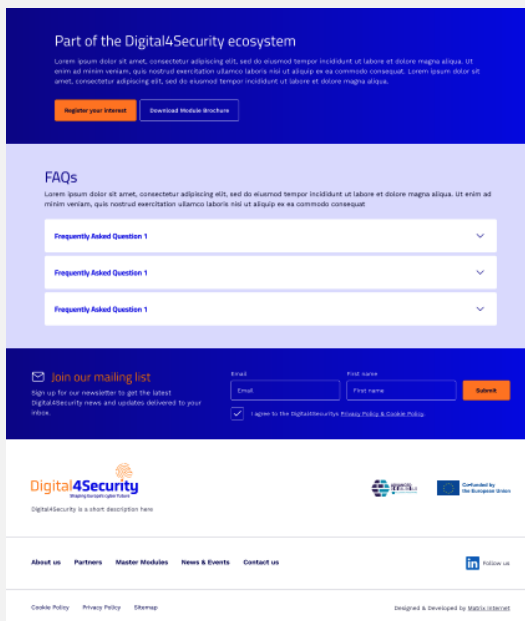


Figure 6: mock-up of design for Module landing page

The table below presents a list of all the module landing page URLs:

Mandatory MODULES	URL
AI and Emerging Topics in Cybersecurity	<a href="https://www.digital4security.eu/module/ai-and-emerging-topics-in-cybersecurity/">https://www.digital4security.eu/module/ai-and-emerging-topics-in-cybersecurity/</a>
Business Resilience, Incident Management and Threat Response	<a href="https://www.digital4security.eu/module/business-resilience-incident-management-and-threat-response/">https://www.digital4security.eu/module/business-resilience-incident-management-and-threat-response/</a>
Cybersecurity Culture, Strategy & Leadership	<a href="https://www.digital4security.eu/module/cybersecurity-culture-strategy/">https://www.digital4security.eu/module/cybersecurity-culture-strategy/</a>
Dissertation / Internship	<a href="https://www.digital4security.eu/module/dissertation-internship/">https://www.digital4security.eu/module/dissertation-internship/</a>
Enterprise Architecture, Infrastructure Design and Cloud Computing	<a href="https://www.digital4security.eu/module/enterprise-architecture-infrastructure-design-and-cloud-computing/">https://www.digital4security.eu/module/enterprise-architecture-infrastructure-design-and-cloud-computing/</a>
Law, Compliance, Governance, Policy, and Ethics	<a href="https://www.digital4security.eu/module/law-compliance-governance/">https://www.digital4security.eu/module/law-compliance-governance/</a>
Research Methods	<a href="https://www.digital4security.eu/module/research-methods/">https://www.digital4security.eu/module/research-methods/</a>
Security Operations	<a href="https://www.digital4security.eu/module/security-operations/">https://www.digital4security.eu/module/security-operations/</a>
Technological Foundations for CS & Security Controls	<a href="https://www.digital4security.eu/module/technological-foundations/">https://www.digital4security.eu/module/technological-foundations/</a>
Elective MODULES	URL
Automation of Security Tasks and Data Analytics	<a href="https://www.digital4security.eu/module/automation-of-security/">https://www.digital4security.eu/module/automation-of-security/</a>
CISO and Crisis Communication	<a href="https://www.digital4security.eu/module/ciso-crisis-communication/">https://www.digital4security.eu/module/ciso-crisis-communication/</a>
Risk Management of Cyber-Physical	<a href="https://www.digital4security.eu/module/risk-management-">https://www.digital4security.eu/module/risk-management-</a>

Systems	<a href="#">cyber/</a>
Cybersecurity Auditing	<a href="https://www.digital4security.eu/module/cybersecurity-auditing/">https://www.digital4security.eu/module/cybersecurity-auditing/</a>
Cybersecurity Economics & Supply Chain	<a href="https://www.digital4security.eu/module/cybersecurity-economics-supply/">https://www.digital4security.eu/module/cybersecurity-economics-supply/</a>
Cybersecurity Education & Training Delivery I	<a href="https://www.digital4security.eu/module/cybersecurity-education-1/">https://www.digital4security.eu/module/cybersecurity-education-1/</a>
Cybersecurity Education & Training Delivery II	<a href="https://www.digital4security.eu/module/cybersecurity-education-training-delivery-ii/">https://www.digital4security.eu/module/cybersecurity-education-training-delivery-ii/</a>
Cybersecurity in Industry - Security of OT and Cyber-Physical Systems	<a href="https://www.digital4security.eu/module/cybersecurity-in-industry/">https://www.digital4security.eu/module/cybersecurity-in-industry/</a>
Cybersecurity Law & Data Sovereignty	<a href="https://www.digital4security.eu/module/cybersecurity-law-data-sovereignty/">https://www.digital4security.eu/module/cybersecurity-law-data-sovereignty/</a>
Machine and Deep Learning in Cybersecurity	<a href="https://www.digital4security.eu/module/machine-deep-learning/">https://www.digital4security.eu/module/machine-deep-learning/</a>
Digital Forensics, Chain of Custody and eDiscovery	<a href="https://www.digital4security.eu/module/digital-forensics-chain/">https://www.digital4security.eu/module/digital-forensics-chain/</a>
Ethical Hacking & Penetration Testing	<a href="https://www.digital4security.eu/module/ethical-hacking-penetration/">https://www.digital4security.eu/module/ethical-hacking-penetration/</a>
Malware Analysis	<a href="https://www.digital4security.eu/module/malware-analysis/">https://www.digital4security.eu/module/malware-analysis/</a>
Threat Intelligence	<a href="https://www.digital4security.eu/module/threat-intelligence/">https://www.digital4security.eu/module/threat-intelligence/</a>

## Digital Marketing Activities

Social media strategy – Partner channels and project LinkedIn page

**Platforms:** Utilises the Digital4Security LinkedIn page, partner social media accounts, campaign landing pages on Full Fabric platform (mydigital4security.eu) and the project blog.

**Content strategy:** Regular posts featuring highlights from the programme, key industry insights, interviews with faculty and students, and updates on cybersecurity trends.

**Engagement tactics:** Polls, and content sharing from partner networks to boost visibility and interaction.

### Email marketing

Digital4Security newsletter:

- **Frequency:** Bi-monthly dispatch to subscribed stakeholders, featuring updates, upcoming events, and spotlight segments on lecturers or notable alumni.
- **Integration:** Links within the newsletter direct subscribers to the website for deeper engagement with content.

- **Template:** a bespoke, on brand template was created within the Brevo email newsletter solution with elements ready to add content for each newsletter edition and can be updated as required depending on the campaign requirements.



Figure 7: example newsletter template element introduction and an element with a CTA to read the full story on the project website



Figure 8: Example of a newsletter template element featuring an animated GIF created by our partners, Indiepics, to engage users. It also includes a CTA directing readers to contact Digital4Security via the programme website for further engagement.

## Webinars and live events

**Setup:** Online webinars, hosted by leading cybersecurity experts, will offer valuable insights into the Digital4Security programme and address pressing industry issues. We plan to organize a minimum of four webinars, as stipulated in the GA and Application Form. Potential topics include 'Cybersecurity Trends in 2025,' 'Protecting Infrastructure from Cyber Threats,' 'Data Privacy Regulations and Compliance,' and 'Advanced Threat Detection Techniques.' These webinars will be promoted through our Digital4Security LinkedIn page, via our newsletter, and across partner social media channels to ensure broad outreach and engagement."

**Live events:** Regional informational sessions at partner universities and industry conferences to provide direct engagement with the programme administrators and alumni.

## Partnerships and collaborations

**Academic Partners:** Collaborate with D4S partner universities across Europe to integrate the Digital4Security curriculum and host joint events such as webinars, networking events, guest lectures etc.

**Industry collaborations:** Work with industry experts (with cybersecurity skills) to ensure the programme meets current industry standards and needs, and to offer practical training opportunities for students.

## Digital Skills and Jobs Platform

As part of our strategic outreach for the Digital4Security Master's Programme launch, we are collaborating with the Digital Skills and Jobs and Platform (DSJP) to enhance visibility and drive engagement among a dedicated community of digital skills advocates and professionals across Europe. Outreach efforts included attending the DSJP drop-in sessions dedicated to the DEP projects, to have a clear overview of the platform and understand how we can promote the master's on their main comms channels, connect with members, recruit students, publish master's resources, and news and events related to D4S.

### 1. Community engagement on DJSP:

We will create a discussion thread within the DJSP Community's private space. This post will highlight key information about the Digital4Security Masters Programme, detailing the unique aspects and opportunities it offers. The initiative aims to attract members who are actively enhancing their digital and cybersecurity skills through the platform.

### 2. Direct communication:

We will share key information about the programme with the DSJP team, who will then send it out via email to all registered DSJP members—over 15,000 individuals—to ensure extensive coverage and participation.

The programme will also be featured in the DJSP's regular newsletter, which has 2,000 subscribers and reaches a broad audience of digital professionals and enthusiasts.

### **3. Promotion on DJSP Training Opportunities page:**

In addition to community posts and direct mail, the programme will be prominently featured on the DJSP's "Training Opportunities" page (<https://digital-skills-jobs.europa.eu/en/opportunities/training>). This will allow us to reach an even broader audience seeking training opportunities in digital skills and cybersecurity).

Digital4Security will have a dedicated landing page with key information on the project and masters; included a direct link to the training/master's.

This collaboration is designed to leverage the extensive reach of the DJSP to not only enhance the visibility of the Digital4Security Masters Programme but also to ensure we are attracting highly motivated and qualified candidates who are actively seeking advancement in their professional capabilities.

## LinkedIn campaign and content strategy



### Digital4Security LinkedIn content strategy

The LinkedIn content strategy for the Digital4Security Masters Programme aims to build awareness, attract prospective students, and establish a professional community around this new educational initiative. By leveraging diverse content types, we will highlight the innovative aspects of the program and engage with a broad audience of cybersecurity professionals and potential students.

#### Content types and posting schedule (subject to revision)

- 1. Insights from instructors: Bi-weekly (every other Monday)**
  - Content focus: Share insights, lessons, and personal experiences from our faculty and course developers to give a behind-the-scenes look at the knowledge and expertise behind our program.
  - CTA: "Discover the expertise behind our cutting-edge curriculum. Learn more about our faculty at [link to faculty page]."
- 2. Programme highlights: Bi-weekly (every other Wednesday)**
  - Content focus: Detail different aspects of the Masters Programme such as module introductions, unique selling points, and application tips.
  - CTA: "Explore how our program can advance your career in cybersecurity. Visit [link to programme page] for more information."
- 3. Event and webinar promotions: As scheduled**
  - Content Focus: Announce upcoming webinars, open days, and virtual info sessions, including details and how to register.
  - CTA: "Join our next event to learn more about our innovative approach to cybersecurity education. Register now at [link to event]."

## Suggested messaging

- Insights from Instructors: "This week's faculty spotlight features [Instructor Name], who will discuss [Topic]. Get a glimpse of the expertise that shapes our curriculum."
- Programme Highlights: "Our programme offers [specific module or feature]. See how it can help you tackle today's cybersecurity challenges. Details at [link]."
- Event and Webinar Promotions: "Don't miss our upcoming webinar on [Topic] this [Date]. Gain valuable insights and ask your questions live. Secure your spot today at [Link]."

## Visual and branding guidelines

- Imagery: Use professional, high-quality images that align with the innovative and tech-forward nature of the programme. Include images of faculty, online learning environments, and cybersecurity visuals.
- Typography and colours: Maintain consistency with the Digital4Security branding guidelines to ensure all posts are easily recognisable and professional.
- Templates: Develop and utilise branded templates for each type of post to streamline creation and maintain a unified look across the campaign.

## Calls to action

- Encourage interactions such as likes, comments, and shares to increase engagement.
- Direct prospective students to the programme's landing page for more detailed information and to initiate the application process.
- Promote registrations for upcoming webinars and events to build a connected and informed community.

## Sample creatives and assets

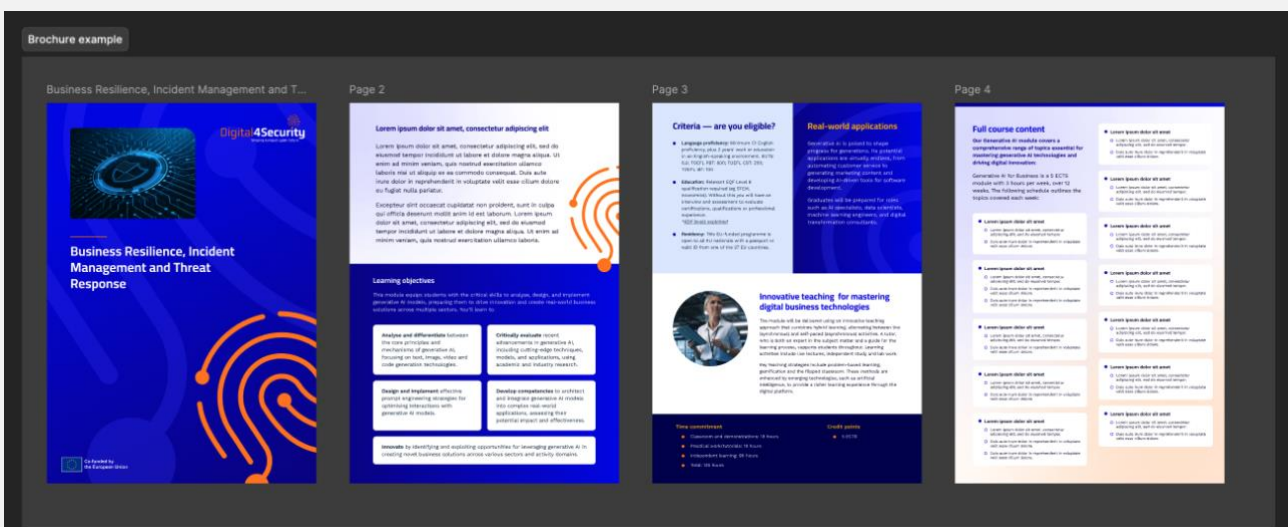


Figure 9: mock-up of brochure design that will be created for each module



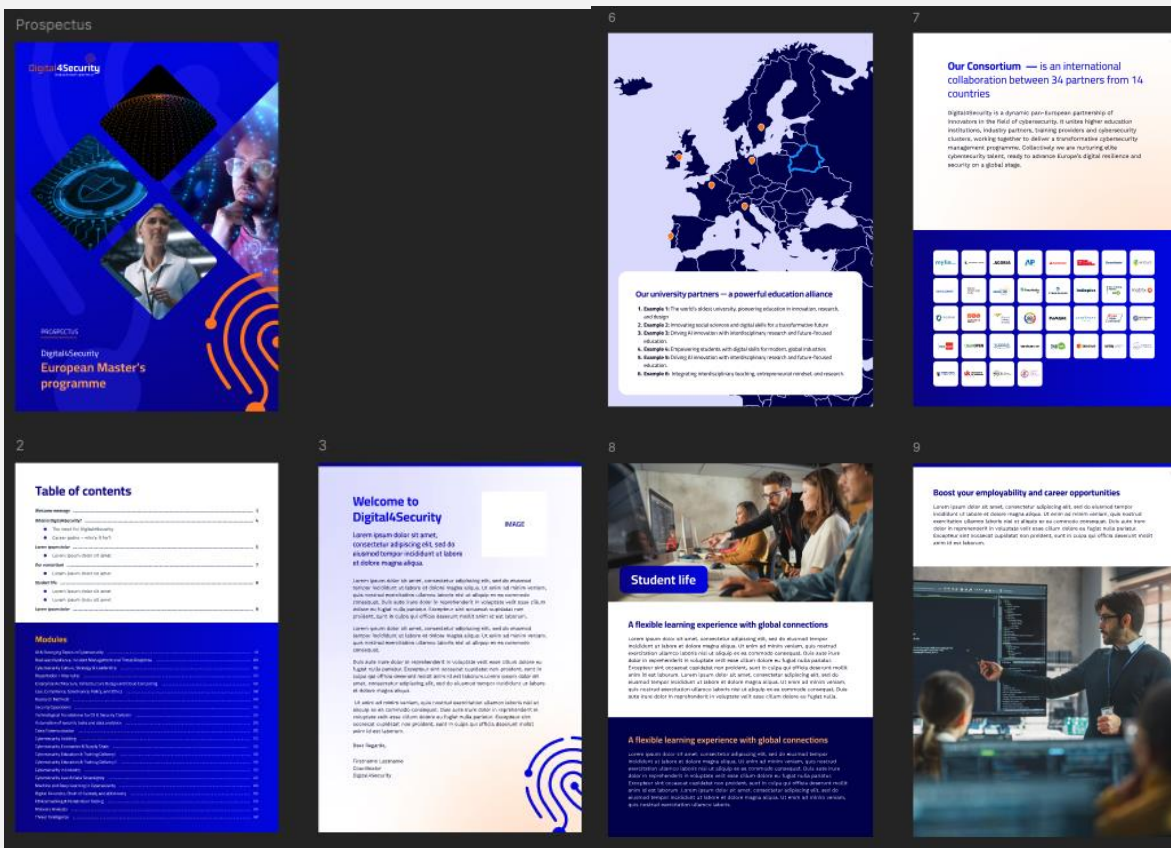


Figure 10: mock-up of prospectus which will include all module brochures

### Sample creatives for campaigns

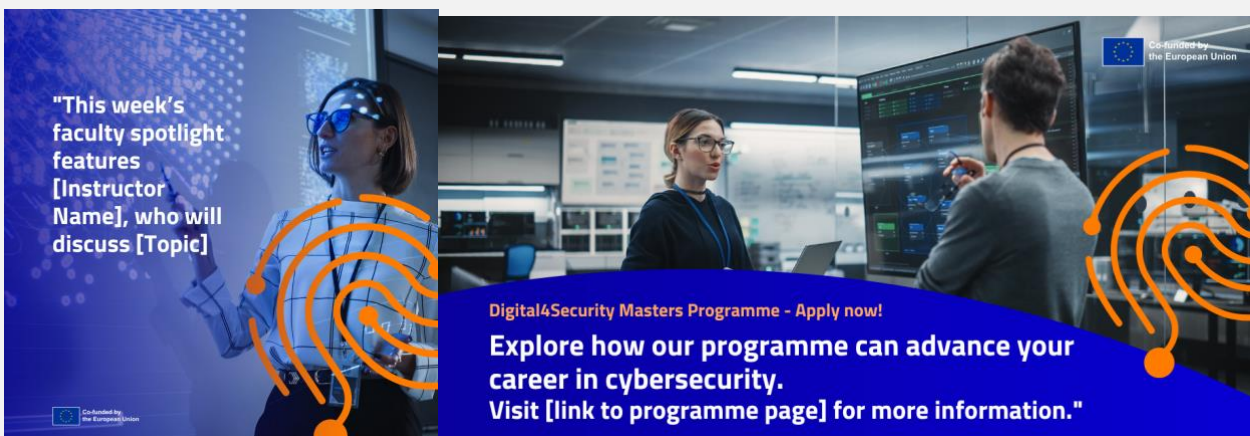


Figure 11: Sample creatives 1 and 2





Figure 12: Sample creatives 3 and 4

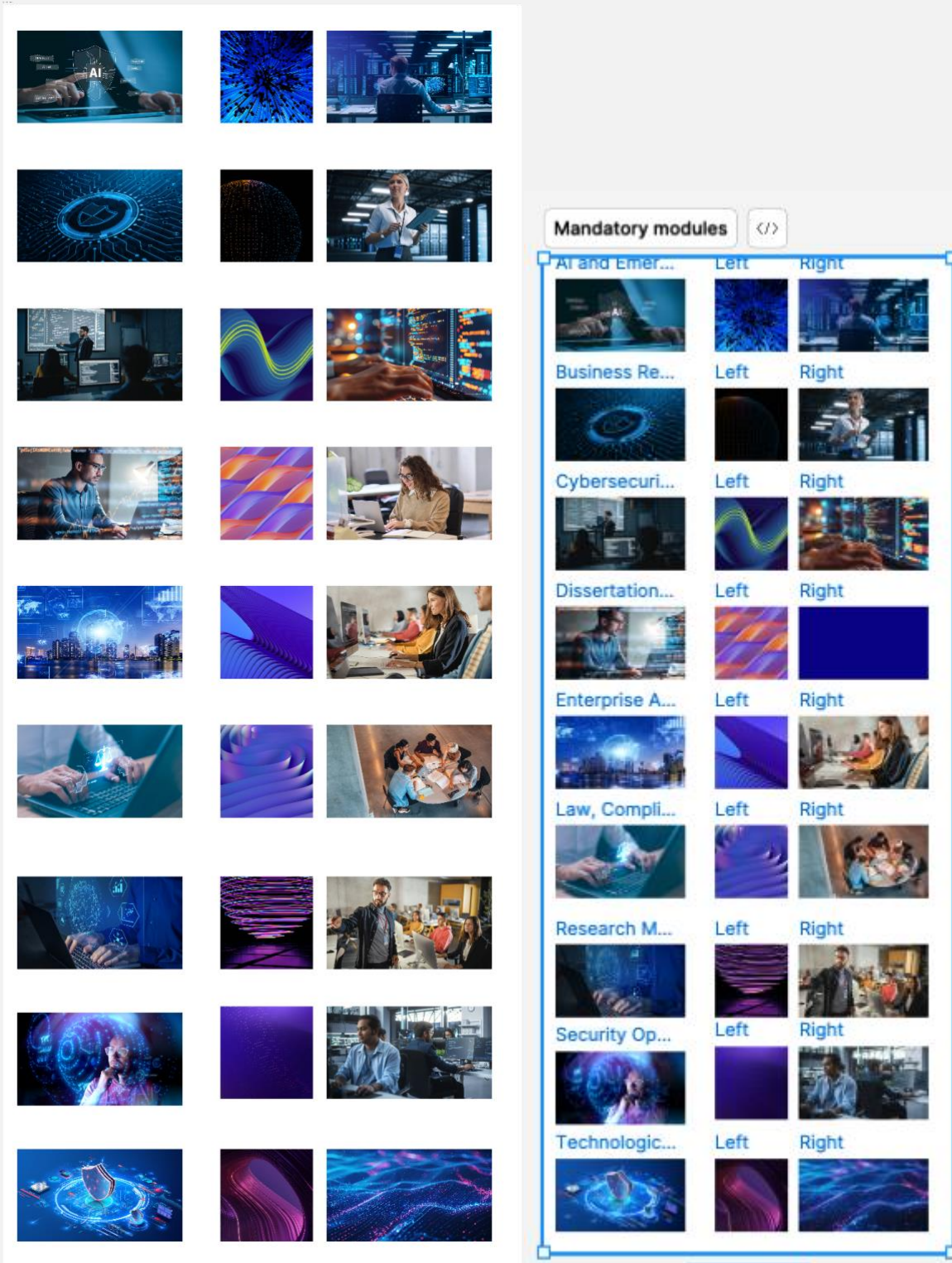


Figure 13: Selected assets for mandatory modules



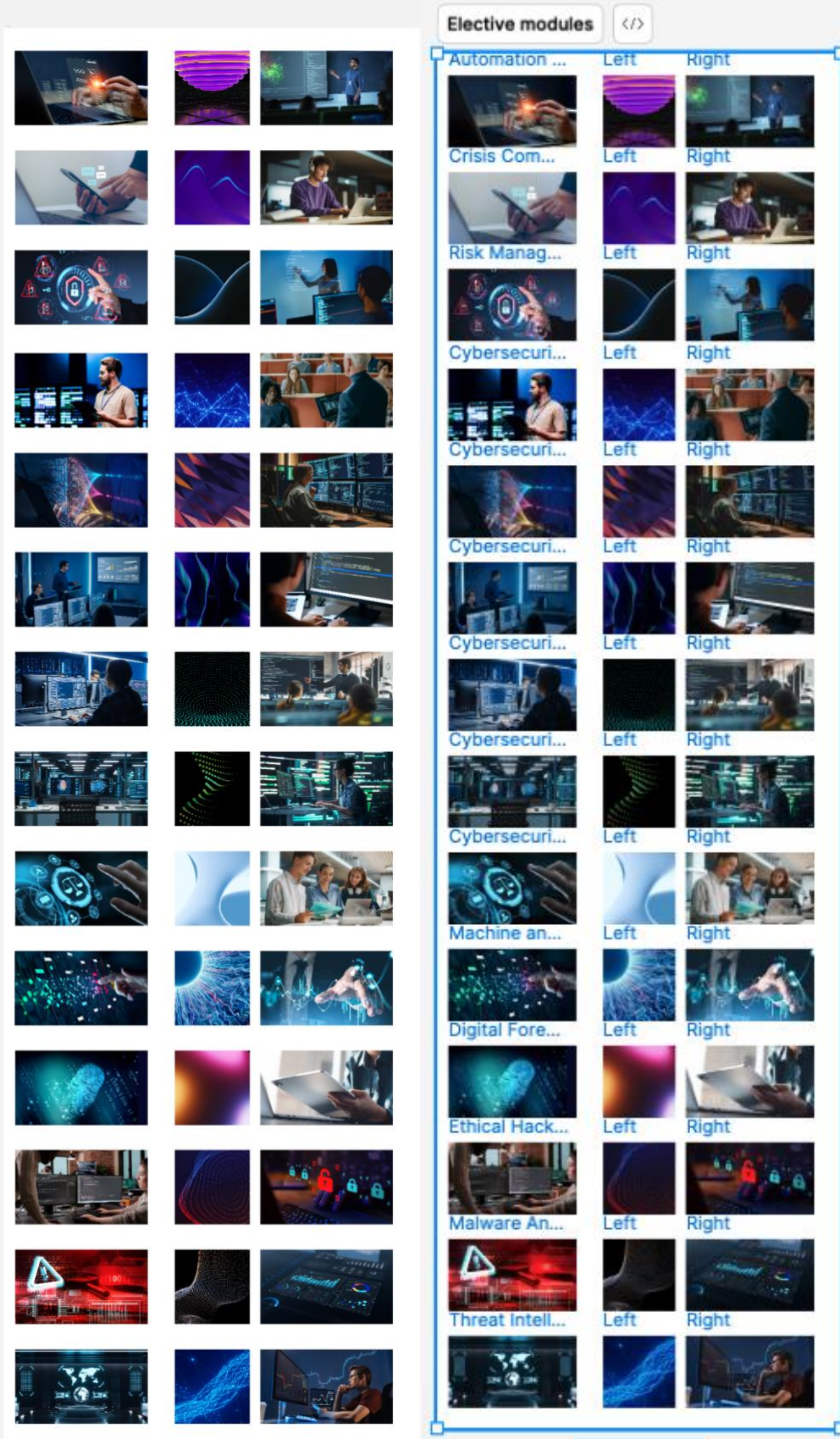


Figure 14: Selected assets for elective modules

## Canva assets

We've templates ready in Canva so that partners can easily adapt and localise as required for targeted campaigns. These include

- Prospectus template
- Flyer template
- Posters A4 template
- Report template
- Brochure template

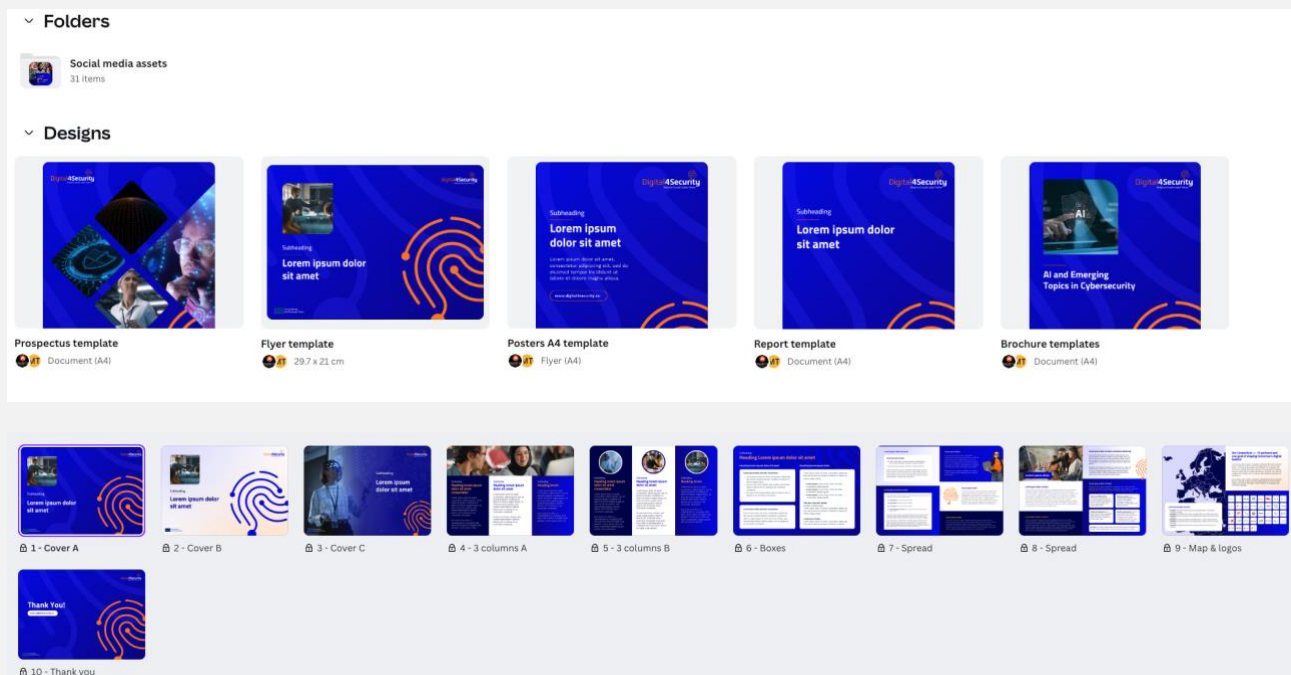


Figure 15: flyer template in Canva that 10 formats

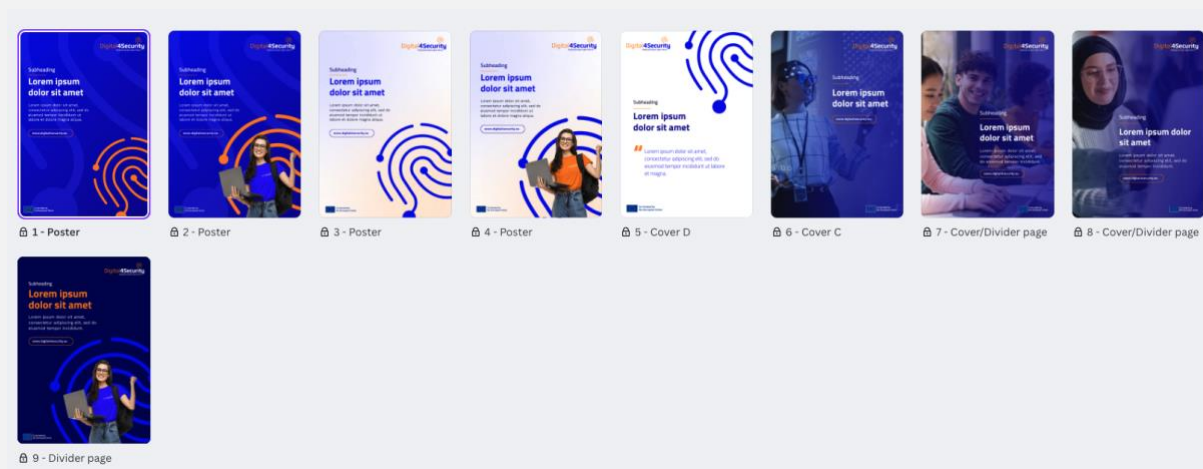


Figure 16: poster template in Canva that has 9 variations



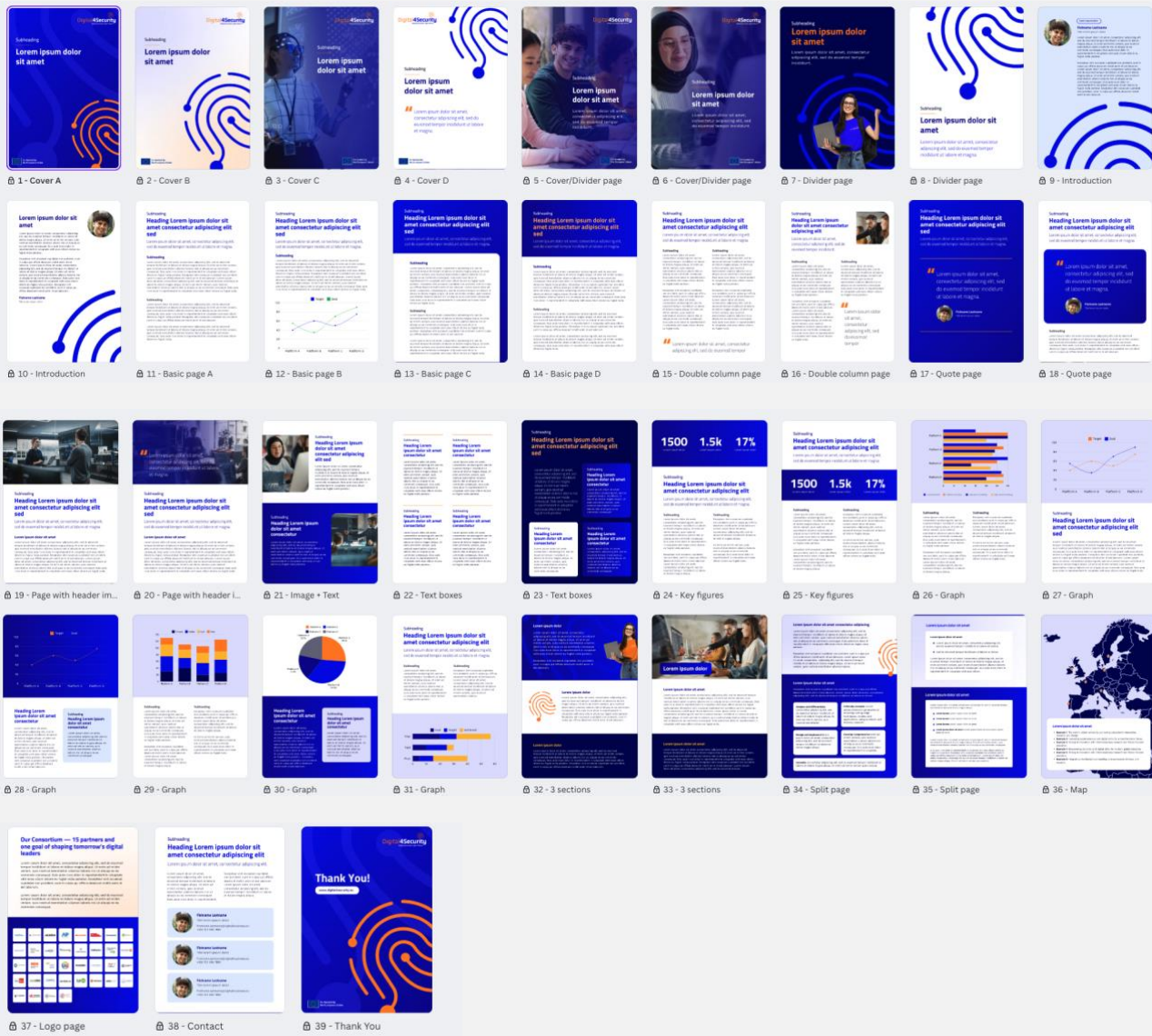


Figure 17: report template in Canva that has 39 different page layouts

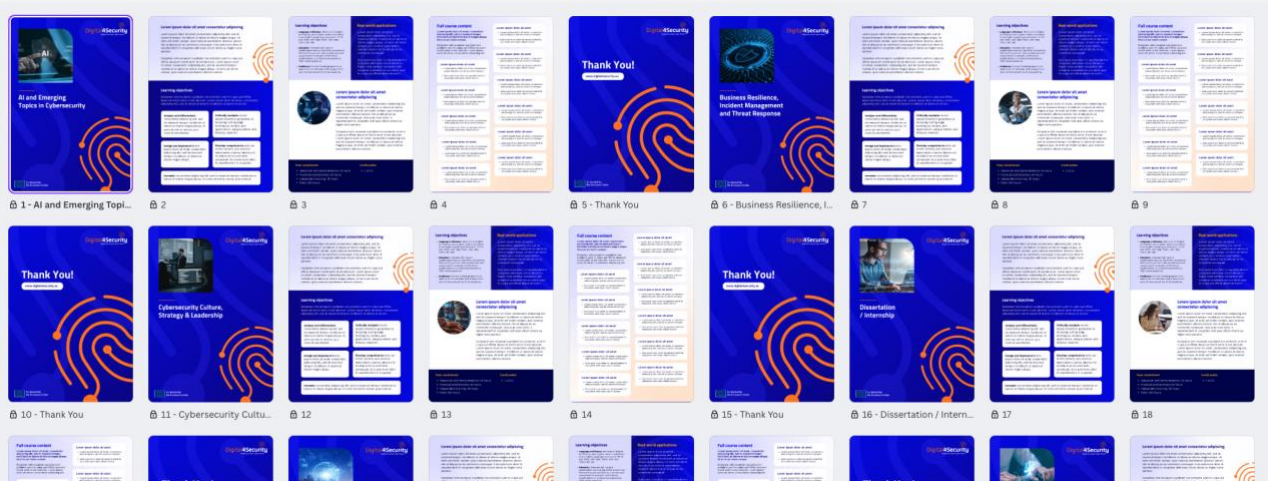


Figure 18: brochure template in Canva that has sections for each module - 115 pages in total

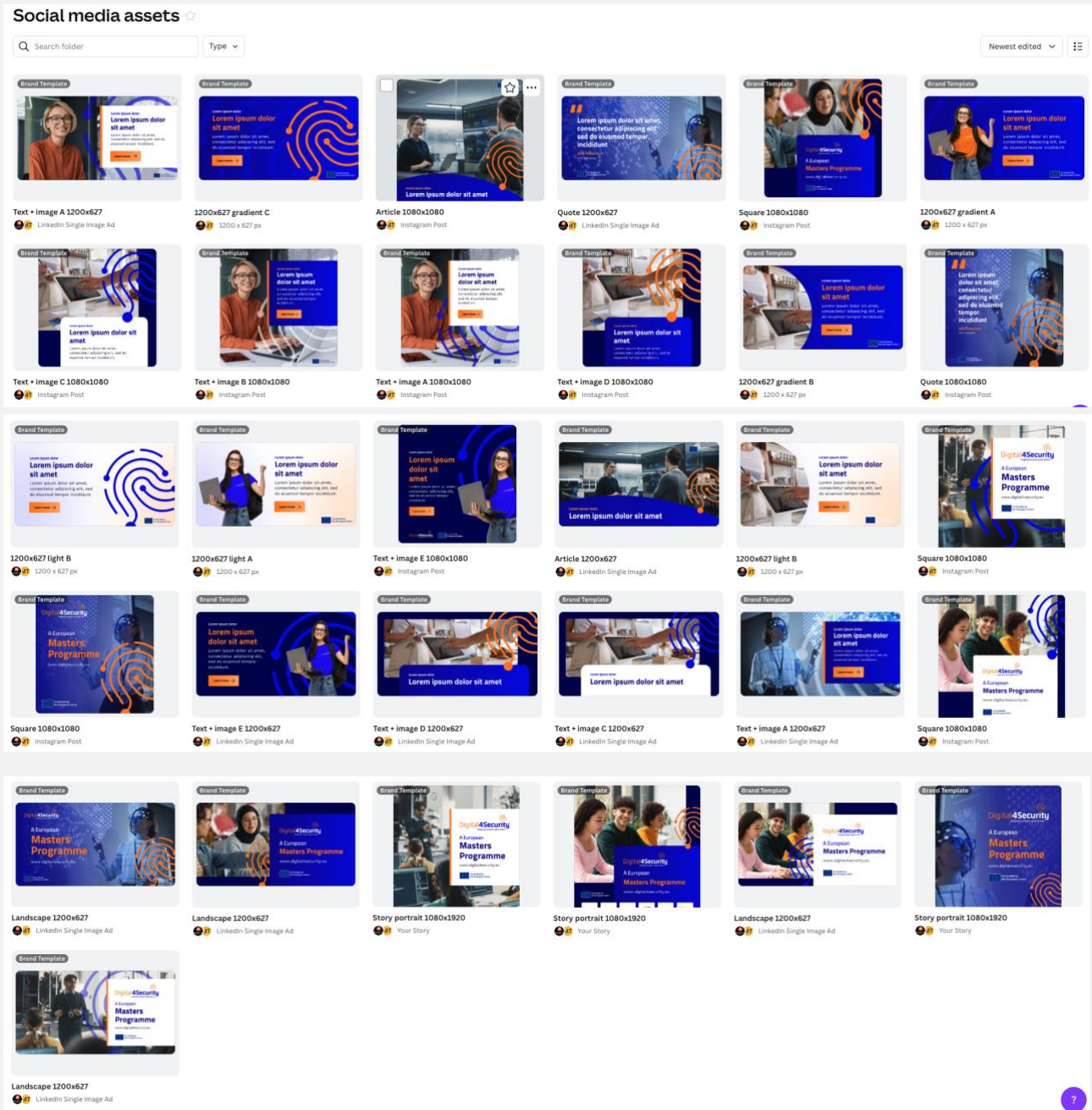


Figure 19: Canva assets ready for partners to localise



## Partner activation packs for the Digital4Security launch campaign

To empower our partners in promoting the Digital4Security Masters Programme, we will provide comprehensive activation packs. These packs are designed to facilitate seamless and effective dissemination of campaign materials across partner channels, ensuring a consistent and localised message reaches diverse audiences.

### Contents of the Activation Packs

#### 1. **Brand and visual identity templates:**

- **Canva templates:** Access to a suite of editable templates on Canva, including posts for social media platforms (Facebook, Instagram, LinkedIn, X), blog banners, and email headers. These templates will adhere to the Digital4Security branding guidelines but allow for customisation to fit local styles and languages.
- **Guidelines document:** Detailed instructions on how to use the templates, including font sizes, colour palettes, and imagery recommendations to ensure brand consistency across all materials.

#### 2. **Content suggestions and templates:**

- **Social media posts:** Pre-written posts with customisable fields to cater to local nuances and specifics. Suggestions for optimal posting times and frequency will be included to maximize reach and engagement.
- **Email and letter templates:** Drafts for emails and letters that can be personalised for different audiences, providing partners with tools to communicate directly with their networks about the programme.

#### 3. **Guidelines for effective sharing:**

- **Best practices document:** A comprehensive guide on how to effectively use different channels (social media, newsletters, blogs) to promote the programme. This will include tips on audience engagement, maintaining dialogue, and leveraging analytics for improved performance.
- **Webinar and event promotions:** Instructions and materials for promoting webinars and other live events, including registration links and speaker information.

#### 4. **Tracking and reporting tools:**

- **Performance tracking sheet:** A simple-to-use digital form to help partners record their outreach activities and measure the impact in terms of engagement and conversions.
- **Feedback and suggestions form:** A method for partners to provide ongoing feedback on the campaign materials and their effectiveness, allowing for continuous improvement.

#### 5. **Promotional multimedia assets:**

- **Images and videos:** High-quality graphics and short video clips that can be used in various promotional contexts to visually engage audiences and convey key messages about the programme.

## Implementation and use

Partners are encouraged to tailor the provided content to resonate with their specific audiences while maintaining the unified messaging crucial to the Digital4Security brand. Each partner will receive access to a digital toolkit on the project SharePoint where all resources can be downloaded and customised.

Partner responsibilities

- **Content localisation:** Partners should adapt the messaging to fit cultural and linguistic needs of their audience, ensuring relevance and increased engagement.
- **Activity tracking:** Partners are expected to track their promotional activities using the provided tools and report back to the Work Package 5 (WP5) leaders on a regular basis.
- **Feedback submission:** Regular submission of feedback on campaign effectiveness and material usability to help refine and optimise ongoing and future marketing efforts.

This structured yet flexible approach allows partners to actively participate in the campaign with the resources needed to engage effectively, while also contributing to the overall success of the programme through coordinated efforts and shared insights.

## Sample content calendar

Digital4Security Launch Campaign: Sample Content Calendar for LinkedIn, YouTube, and Blogs

Week 1: Introduction and Awareness

- **Monday, Week 1**
  - **Content:** Introduction to the Digital4Security Masters Programme
  - **Platform:** LinkedIn, Blog
  - **CTA:** "Discover the future of cybersecurity education. Visit our website to learn more!"
  - **Description:** A blog post providing a high-level overview of the programme and its unique value proposition.
- **Wednesday, Week 1**
  - **Content:** Webinar Announcement: "Meet Your Instructors"
  - **Platform:** LinkedIn
  - **CTA:** "Register for our upcoming webinar to meet the instructors and learn directly about the curriculum!"
  - **Description:** Promote the first interactive webinar with a link to a registration landing page.
- **Friday, Week 1**



- **Content:** Introduction Video on YouTube
- **Platform:** YouTube
- **CTA:** "Watch our introductory video to see what the Digital4Security Masters Programme has to offer you."
- **Description:** A YouTube video introducing the programme, featuring interviews with faculty and highlighting the curriculum's benefits.

## Week 2: Programme Highlights and Engagement

### ● Monday, Week 2

- **Content:** Highlight of a Key Programme Feature: Real-World Case Studies
- **Platform:** LinkedIn
- **CTA:** "Explore how our real-world case studies prepare you for a career in cybersecurity. Learn more on our LinkedIn page."
- **Description:** A post focusing on the hands-on learning experiences included in the programme.

### ● Wednesday, Week 2

- **Content:** Faculty interview on YouTube
- **Platform:** YouTube
- **CTA:** "Gain insights from our top faculty about the cybersecurity landscape. Subscribe to our YouTube channel for more expert views!"
- **Description:** A video interview with one of the programme's leading instructors discussing industry trends and programme benefits.

### ● Friday, Week 2

- **Content:** Blog post: "Cybersecurity in the modern world"
- **Platform:** Blog
- **CTA:** "Read our latest blog post to understand the evolving challenges in cybersecurity."
- **Description:** A detailed article discussing current cybersecurity challenges and how the programme prepares students to address these issues.

## Week 3: Deep dive into curriculum and interaction

### ● Monday, Week 3

- **Content:** Live Q&A session announcement
- **Platform:** LinkedIn
- **CTA:** "Have questions about our master's programme? Join our live Q&A session this Friday!"
- **Description:** Announce an upcoming live Q&A on YouTube, inviting prospective students to interact directly with programme coordinators.

### ● Wednesday, Week 3

- **Content:** Insight into the cybersecurity curriculum
- **Platform:** LinkedIn
- **CTA:** "Dive deeper into our dynamic cybersecurity curriculum. Discover how we equip you with the skills to succeed!"

- **Description:** A LinkedIn post providing an overview of the curriculum's unique features and benefits, engaging prospective students with content about educational outcomes.
- **Friday, Week 3**
  - **Content:** In-depth programme analysis
  - **Platform:** Blog
  - **CTA:** "Delve deeper into what makes our cybersecurity programme a leader in the field. Visit our blog for a comprehensive analysis."
  - **Description:** A blog post that provides an in-depth look at the programme's curriculum, faculty, and student support services.

Week 4: Final push for applications

- **Monday, Week 4**
  - **Content:** Application deadline reminder
  - **Platform:** LinkedIn
  - **CTA:** "Don't miss out! The application deadline for the Digital4Security master's programme is this week. Apply now!"
  - **Description:** A final call to action to encourage applications before the deadline.
- **Wednesday, Week 4**
  - **Content:** Last call for applications
  - **Platform:** LinkedIn
  - **CTA:** "Last chance to apply! Our application deadline is approaching fast. Make sure to submit your application today!"
  - **Description:** A LinkedIn post summarising the programme benefits and urging viewers to apply before the deadline.
- **Friday, Week 4**
  - **Content:** Blog post: "Why choose Digital4Security?"
  - **Platform:** Blog
  - **CTA:** "As the application deadline approaches, discover why the Digital4Security master's programme should be your top choice for cybersecurity education."
  - **Description:** A persuasive blog post aimed at undecided applicants, highlighting the unique selling points and long-term benefits of the programme.

## Recruitment and onboarding



### Enrolment goals and targets

The Digital4Security Masters Programme aims to train a minimum of 2,500 students throughout the duration of the project. The programme seeks to achieve a balanced intake each year, focusing on diversity in terms of gender, geographical representation, and professional background to build a robust cohort of cybersecurity experts. Specific targets include:

- Minimum 3000 applicants from at least the 15 EU countries covered by the consortium
- Minimum 2500 students enrolled in the D4S Masters Programme. (D4S 1 Full time masters programme = 200, D4S 2 Part time = 400) Intake 1 = 600 students, Intake 2 = 850 students, Intake 3 = 1050 students
- Minimum 1000 SMEs/companies with existing staff enrolled in D4S.
- Increasing female enrolment to at least 40% of the student body each year.
- Ensuring representation from at least 75% of participating countries.
- Recruiting a significant number of students from non-ICT backgrounds to diversify the skill sets within the cybersecurity field.

### Recruitment Channels

To effectively reach potential candidates, Digital4Security will utilise a variety of channels for recruitment and onboarding:

#### Digital Platforms:

##### 1. Information gathering

The Master's website will host all the information about the programme, such as eligibility requirements and pricing. The general public will be able to get all necessary information at [www.digital4security.eu/](http://www.digital4security.eu/) including video introductions to modules,

instructor interviews, and student testimonials. Interactive webinars and virtual open days will allow direct engagement with prospective students.

## 2. Application process

When prospective students are ready to apply, they will follow the application link on the website, which directs them to the Full Fabric student enrolment platform. The application process will be accessed via [my.digital4security.eu](https://my.digital4security.eu), which will also serve as the main student dashboard.

3. **Interacting as a student** [learn.digital4security.eu/](https://learn.digital4security.eu/) is the Moodle LMS platform where students will be enrolled once their application is approved and where all courses will take place. By default, students will access the whole platform via <https://my.digital4security.eu>, which will link to individual courses hosted on the LMS at <https://learn.digital4security.eu>.

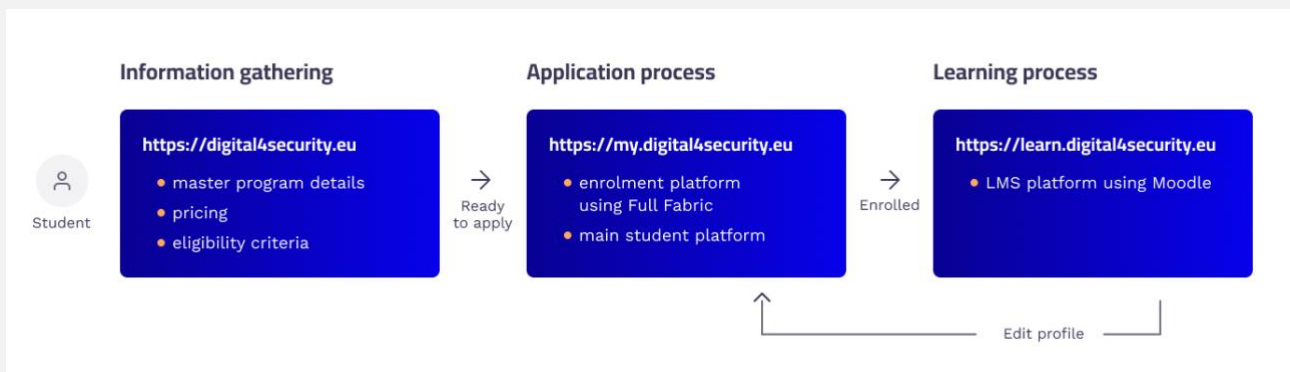


Figure 20: Student journey across Digital4Security Digital platforms

**Social media and online marketing:** Targeted ads and organic posts on platforms like LinkedIn, Facebook, and Instagram will be used to increase program visibility and drive website traffic.

**Educational fairs and conferences:** Representatives from Digital4Security will attend relevant educational and industry events to promote the program and engage with potential students directly.

**Partnerships with educational institutions:** Collaborations with universities and training institutes to offer informational sessions and workshops that highlight the benefits of the programme.

## Engagement with high schools, universities, and industry associations

Digital4Security will actively engage with educational and professional organisations to foster interest and streamline pathways into the cybersecurity field:

**Universities:** Partnerships to create pathways for undergraduate students into the Masters Programme, including credit transfer agreements and co-hosted seminars. We aim to recruit 12

HEIs as Associate Partners during the project who will offer the full or part-time programme from Y5.

**Industry associations:** Collaborations to align the curriculum with industry needs and trends, ensuring graduates are job-ready. These partnerships will facilitate internships, mentorships, and job placements for students. We aim to recruit 40 new industry partners to join the consortia as associate partners and sign cooperation agreements during the project duration.

## Full Fabric admission and enrolment

Full Fabric<sup>1</sup> is a comprehensive admissions and enrolment platform that streamlines the process of recruiting, admitting and enrolling students at scale.

### Full Fabric includes the following basic blocks:

1. “Foundation” CRM system;
2. “Origin” admissions system;
3. “Core” student information system.

Full Fabric handles the entire student user experience and workflows outside of the learning content, which is managed by the Moodle LMS system.

### Full Fabric covers the following aspects of the user journey:

- Eligibility process;
- Student application;
- Onboarding;
- Remarketing and reminders (GDPR-compliant);
- Course enrolment;
- Student dashboard and links to LMS.

## Embedded Full Fabric forms on project website

Full Fabric enables us to embed custom forms on the project that enables all submissions to be captured in Full Fabric in one centralised location where we can send targeted campaigns to prospective students. Here is an example of a live form to capture interest from prospective students: <https://www.digital4security.eu/register-you-interest/>

---

<sup>1</sup> <https://www.fullfabric.com/>

**Digital4Security**  
Shaping Europe's cyber future

## Register your interest

First name\*

Last name\*

Email address\*

Which modules are you interested in\*

What type of course format are you interested in?

Select ▼

Would you be interested in participating in a pilot programme?

Select ▼

How did you hear about Digital4Security

**Privacy policy\***  
We will use your data throughout your student journey, and may share it with third parties as needed for this purpose. For more details, please review our [Privacy Policy here](#).

I accept the Privacy policy

**Marketing policy\***  
Please opt in to receive more information and offers on our academic programmes

I would like to receive information by email

I do not want to be contacted with this type of information

**Submit**

Figure 21: shows a UI mock-up the 'Register Your Interest' form.

**Digital4Security**  
Shaping Europe's cyber future

About Digital4Security Partners News & Events Get in Touch **Register Your Interest**

## Shaping Europe's cyber future

Digital4Security is a pioneering pan-European master's programme in cybersecurity management and data sovereignty. Close the cybersecurity skills gap by joining a new wave of experts, blending practical industry insights with academic excellence.

Take the first step towards safeguarding Europe's digital landscape.

**Get early access**



Figure 22: shows the registration form embedded on the project website linked to on the main navigation on all website pages via a 'Register Your Interest' CTA

Admissions/enrolment process narrative

**Step 1:** The applicant visits the client website and clicks “Apply now,” or clicks the “Apply now” call to action in an email.

**Step 2:** The applicant is redirected to the Full Fabric platform’s [Home Page](#), where they receive instructions on the application process.

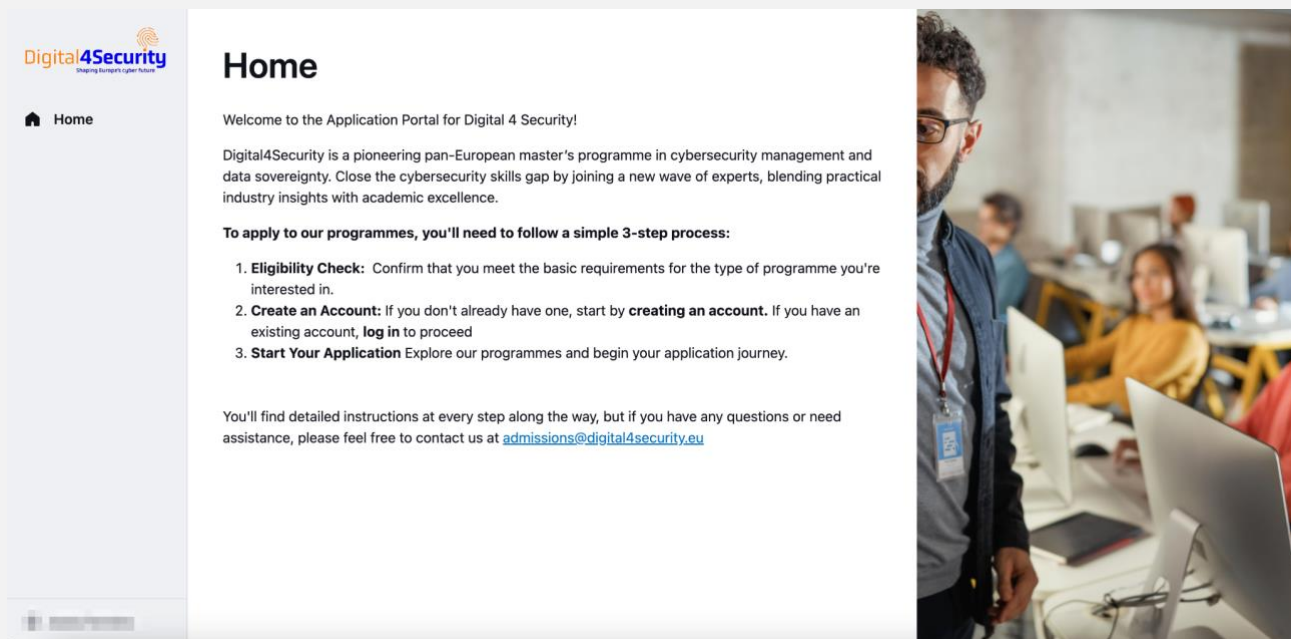


Figure 23: Full Fabric home page

**Step 3** Applicant [Signs Up/Logs In](#) to the portal:

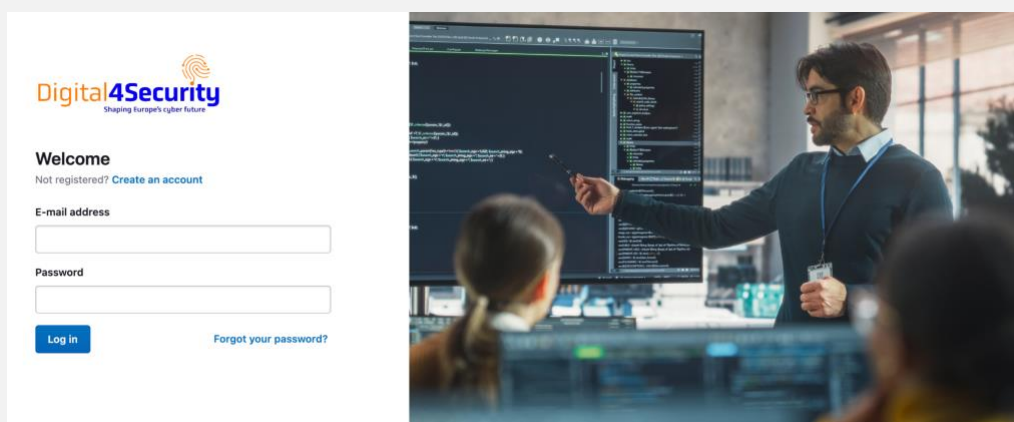


Figure 24: Full Fabric login page

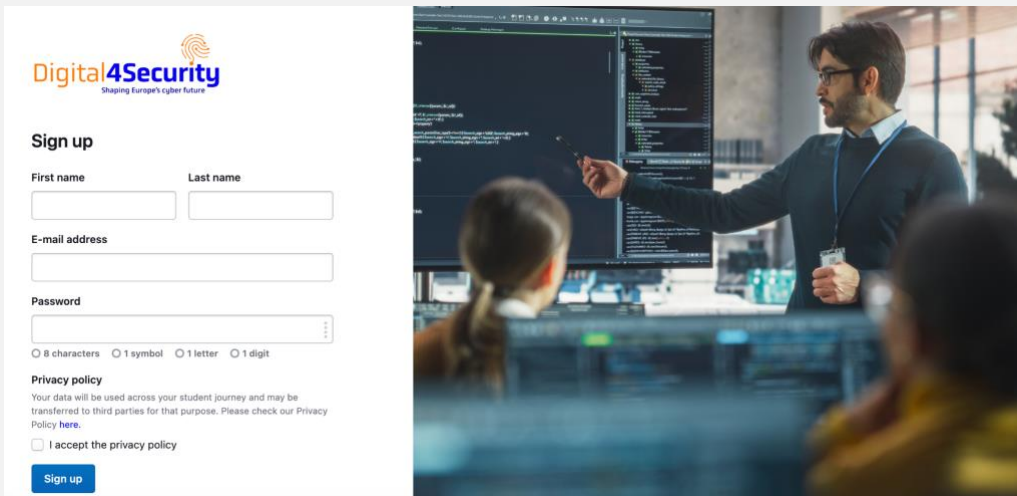


Figure 25: Full Fabric Sign up page

**Step 4** Applicant completes the Eligibility Assessment for Digital4Security's programmes (selecting the programmes they are interested in)

### Result 1: Eligibility assessment — PASS

The applicant immediately receives an automated email confirming their eligibility to apply to the programme – State: Prospect\_pass\_eligibility.

YES: Applicant receives an email confirming they can now apply to the programme. — Prospect\_pass\_eligibility

If **PASS/YES** - Applicant navigates to the relevant page to start/continue application:

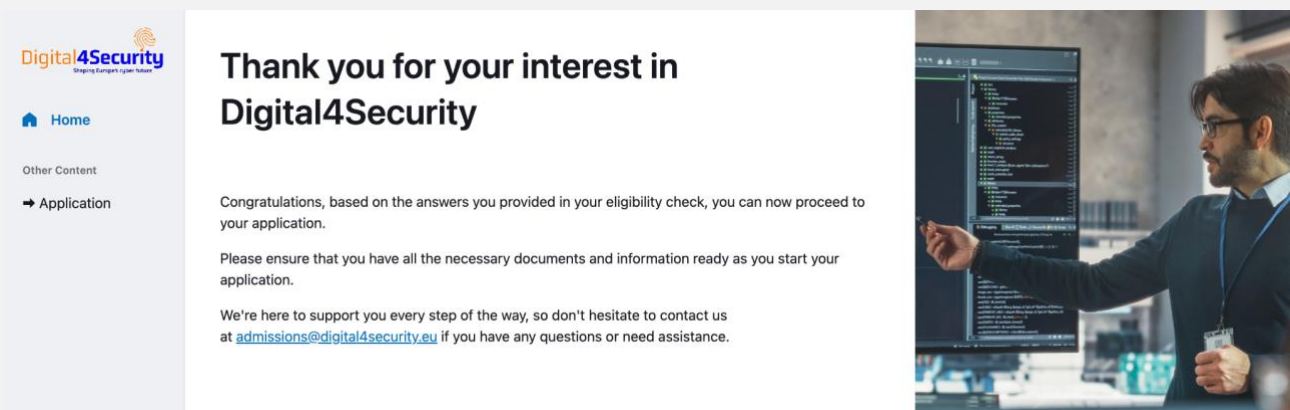


Figure 26: Confirmation Page



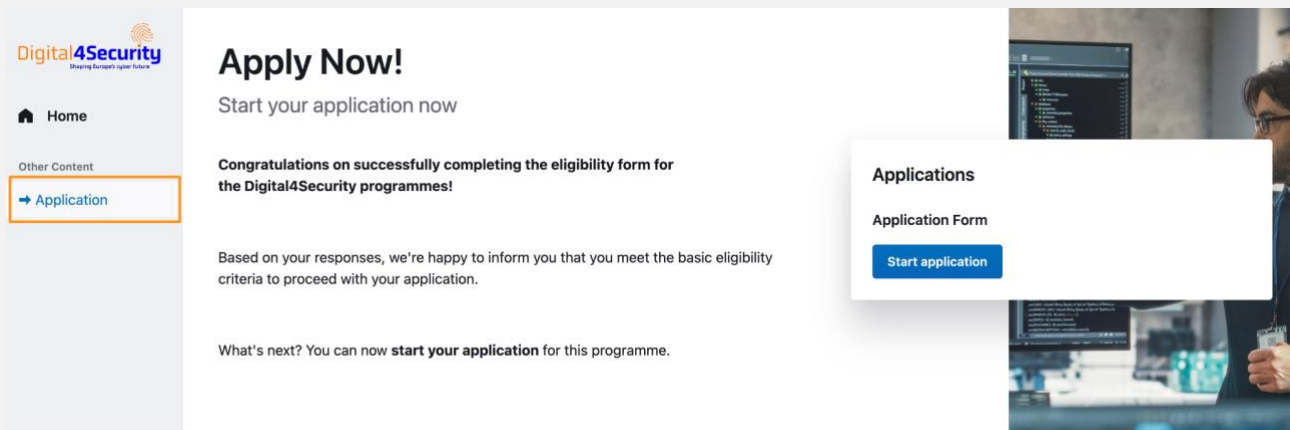


Figure 27: Start Application page

## Result 2: Eligibility Assessment - FAIL

State: Prospect\_fail\_eligibility – The prospect has submitted and failed the eligibility assessment.

**NO:** Applicant receives rejection email. — Prospect\_fail\_eligibility

**Step 5:** Applicants validate their email address through a link received automatically by email.

**Step 6:** The applicant starts the application process and fills out all required information – State: Prospect\_started\_application.

Each tab of the application form includes the necessary questions and uploads for the applicant to complete their submission. The form's content is fully customisable and can be updated at any time.

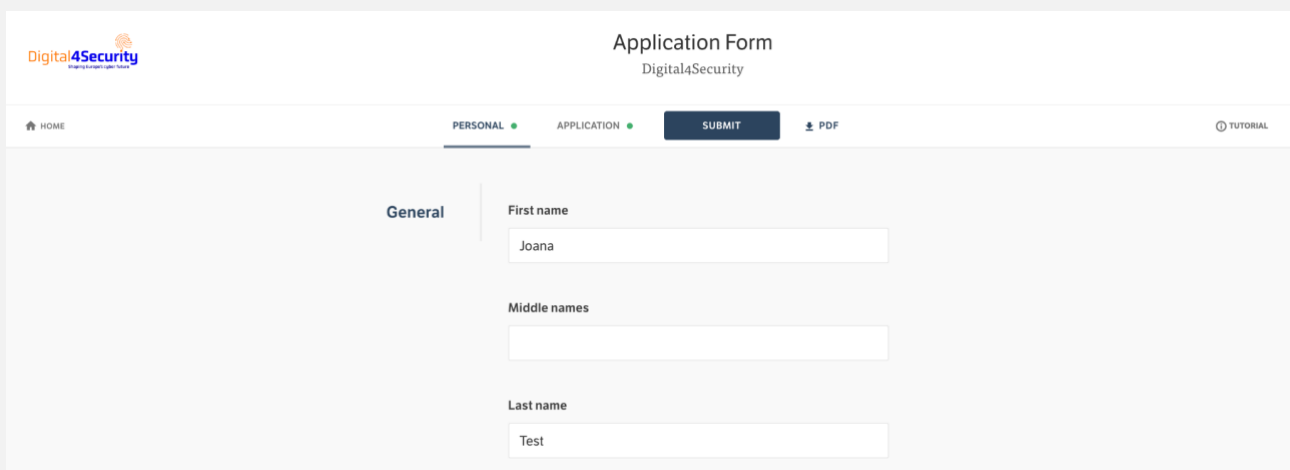


Figure 28: Application form

**Step 7:** The applicant submits the application form – An automated confirmation email is sent to the applicant, and a notification is sent to the admissions team to review the application – State: Applicant\_submitted.

**Step 8:** The admissions team reviews the submitted application forms using evaluation criteria to ensure the applicant's profile meets the programme's admission requirements.

## Full Fabric Process Diagram

Figure: outcome of the process mapping workshop

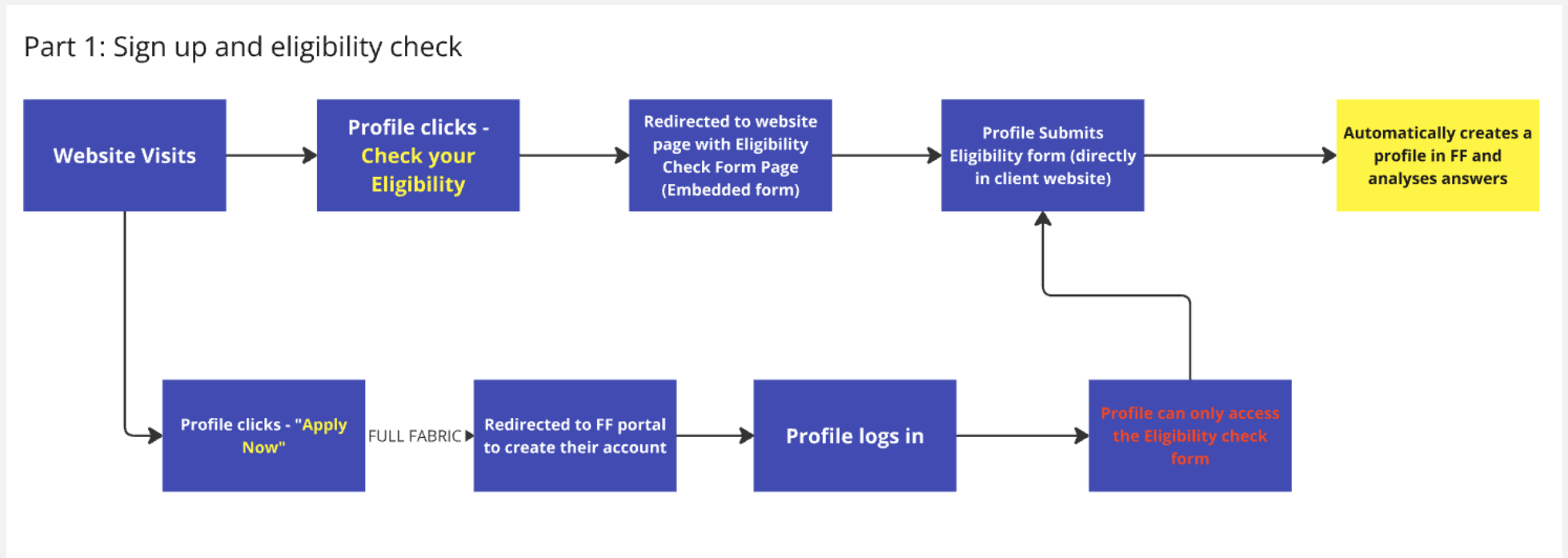


Figure 29: the sign up and eligibility check process

Part 2: Application outcome

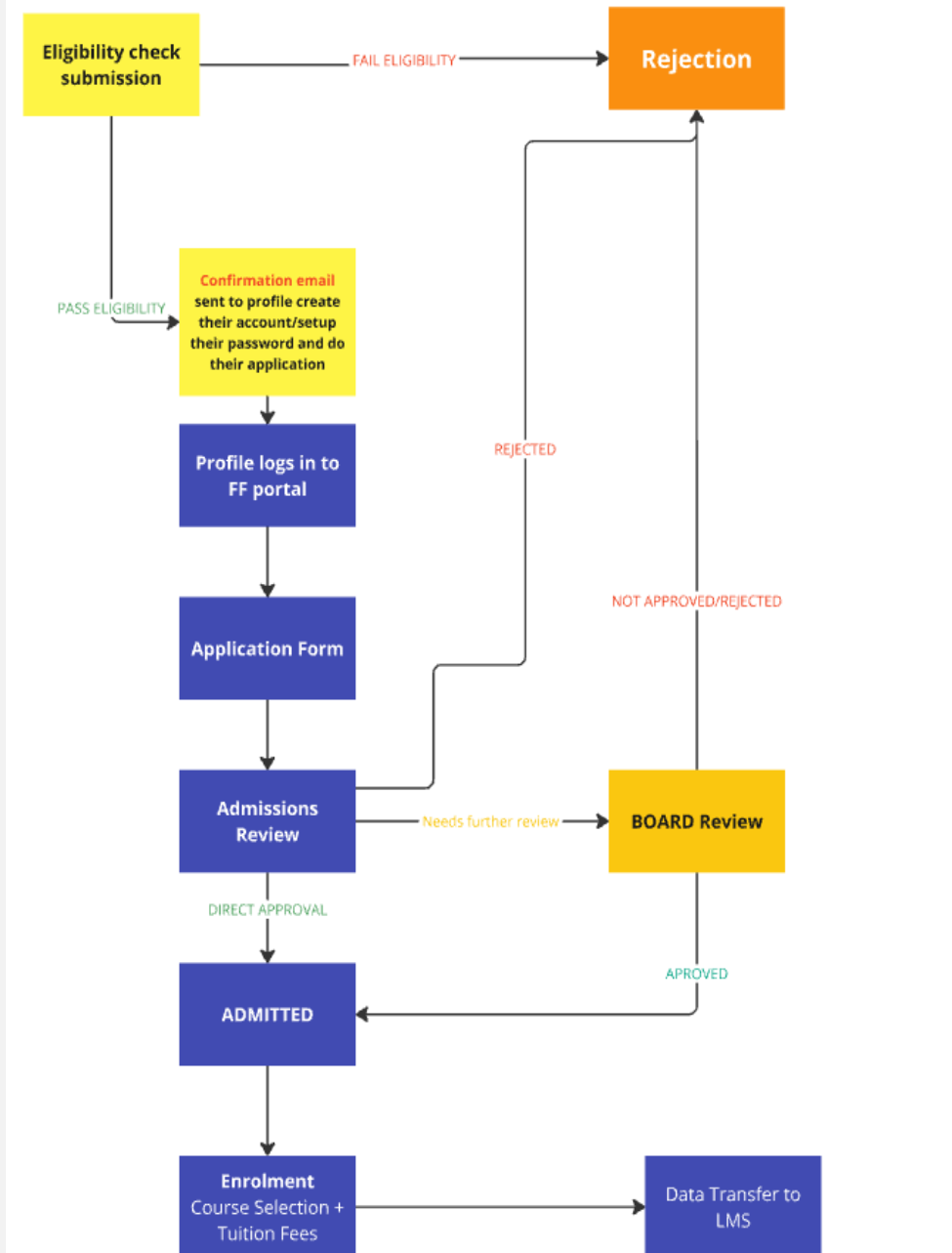


Figure 30: student application application process flow

## Emails

Full Fabric offers a suite of automated emails that can be configured with customisable messages that can be sent as required. The brand guidelines have been applied and the template is as follows:

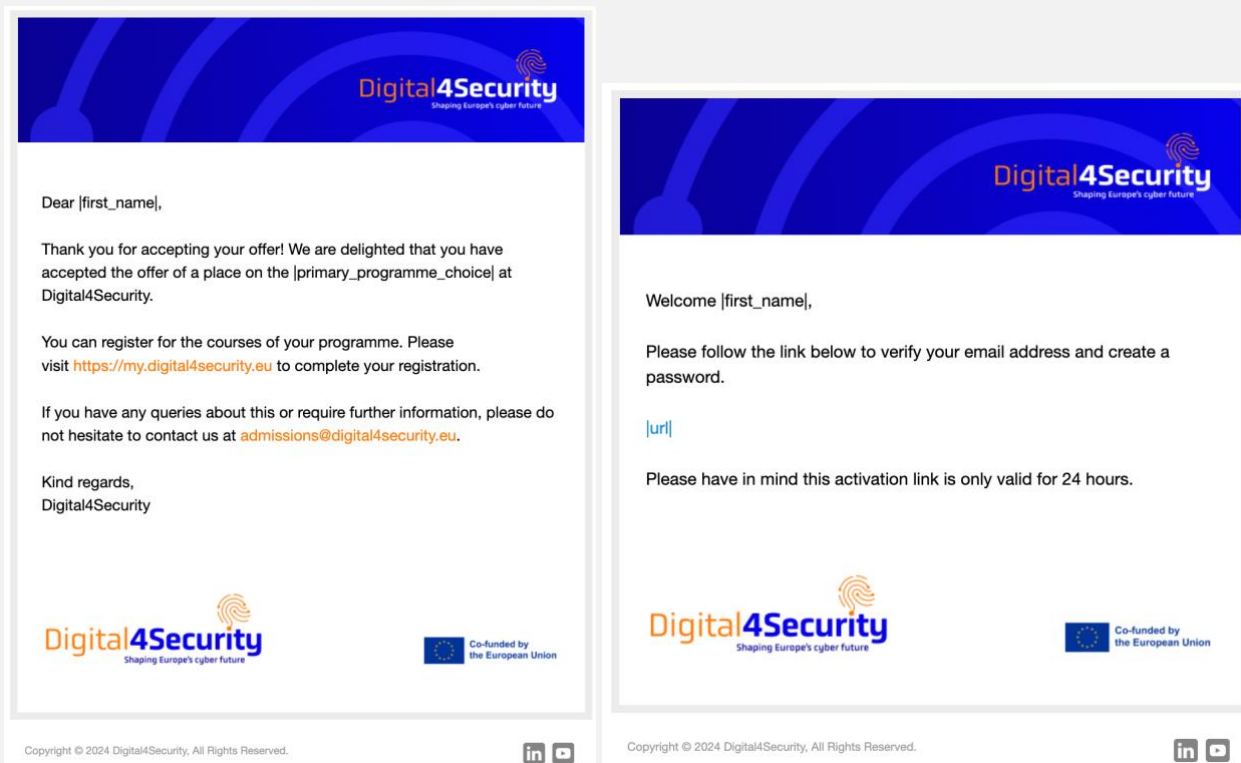


Figure 31: Automated emails

We are currently working on the student registration form for the pilot:

<https://my.digital4security.eu/templates/672107073b5d000b7e88249e/start>

Applicant accesses the admissions' portal:

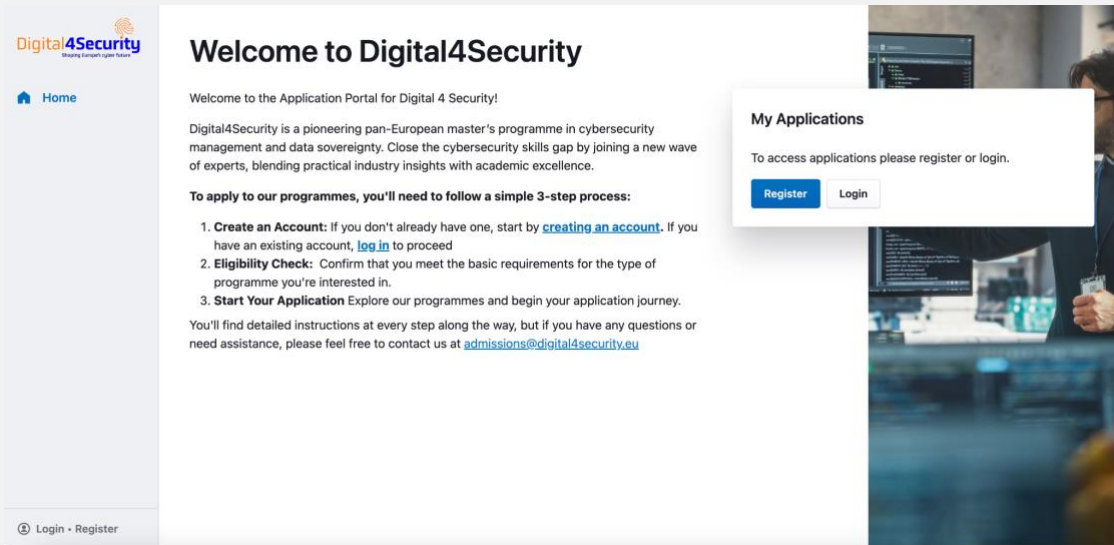


Figure 32: Applications portal

Applicant creates an account/logs in:

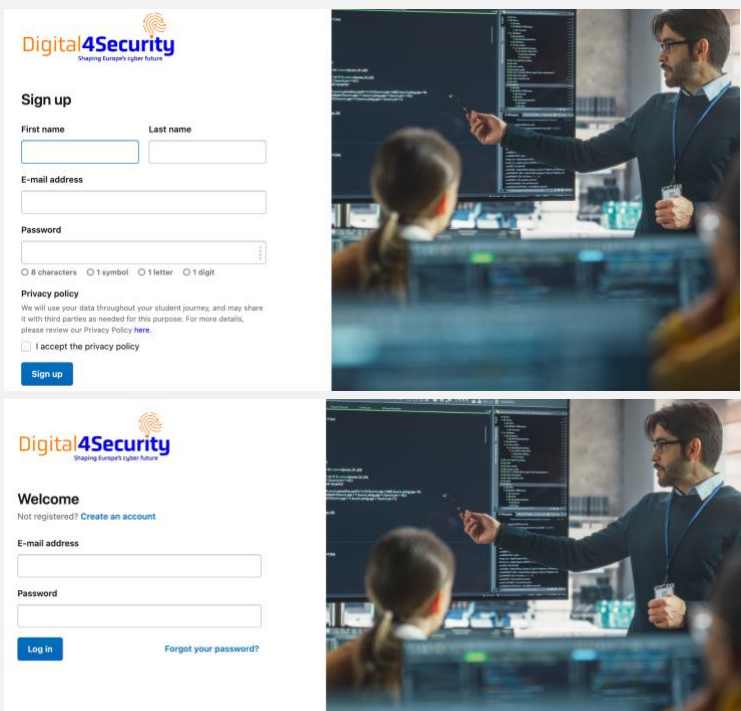


Figure 33: Create account / login screen

This is what the applicant will see once logged in:

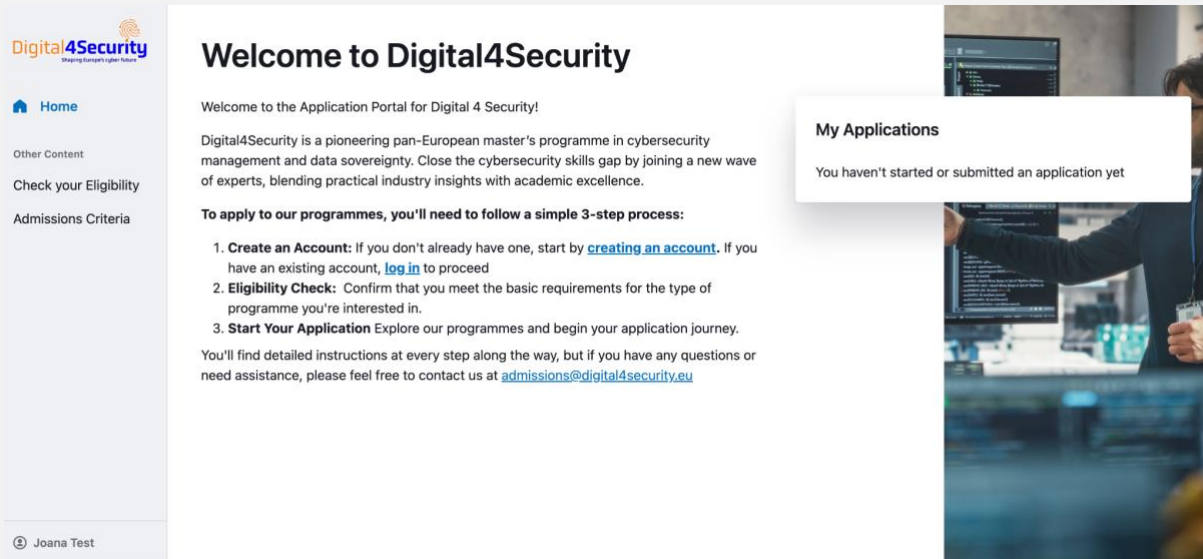


Figure 34: My applications

Admissions Criteria Page:

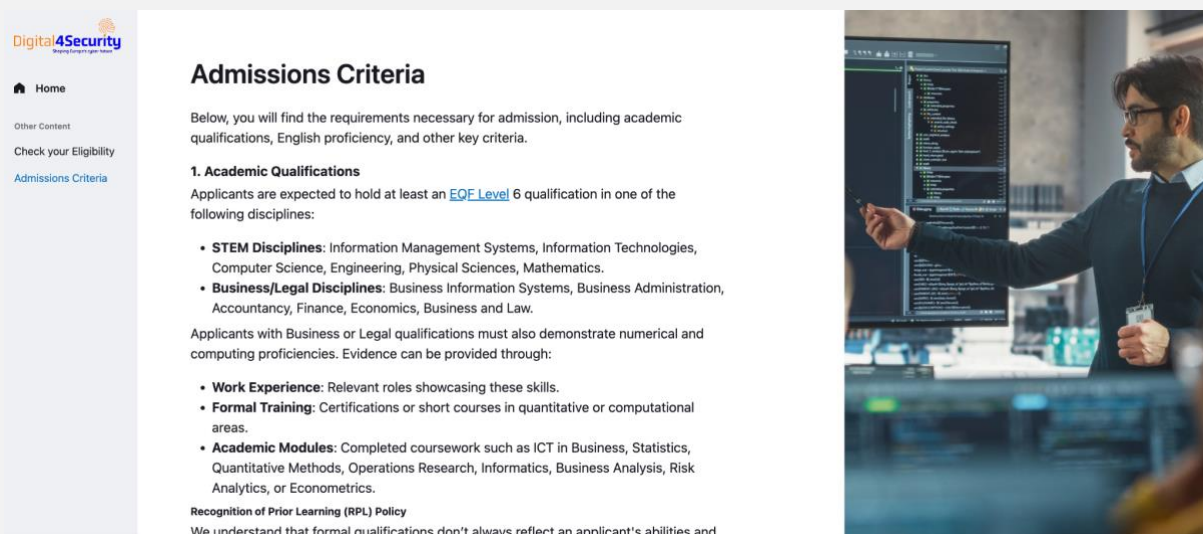


Figure 35: Admissions criteria

Eligibility PASS:

- Page:

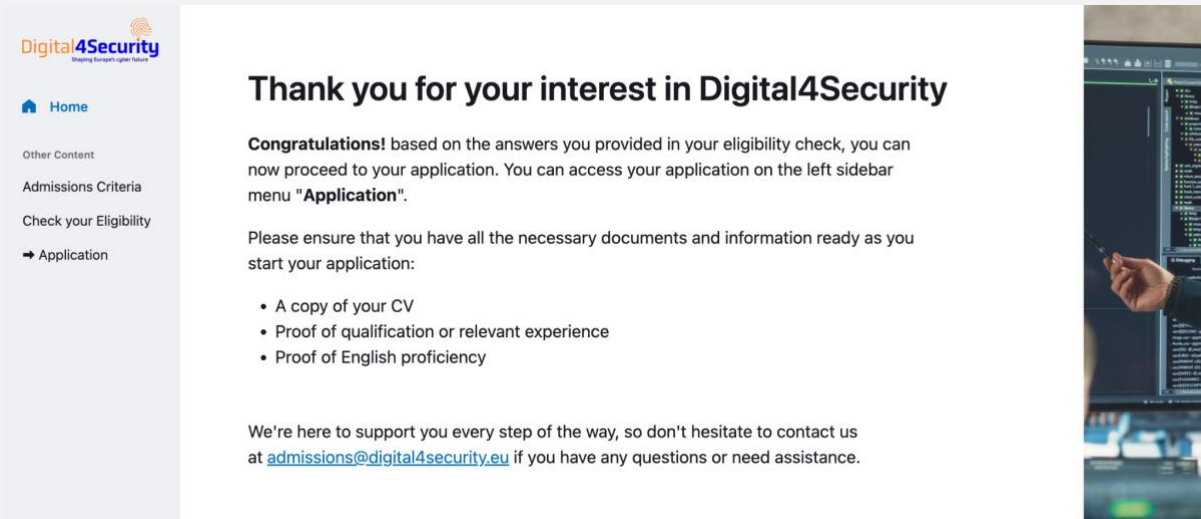


Figure 36: Eligibility check

- Email:

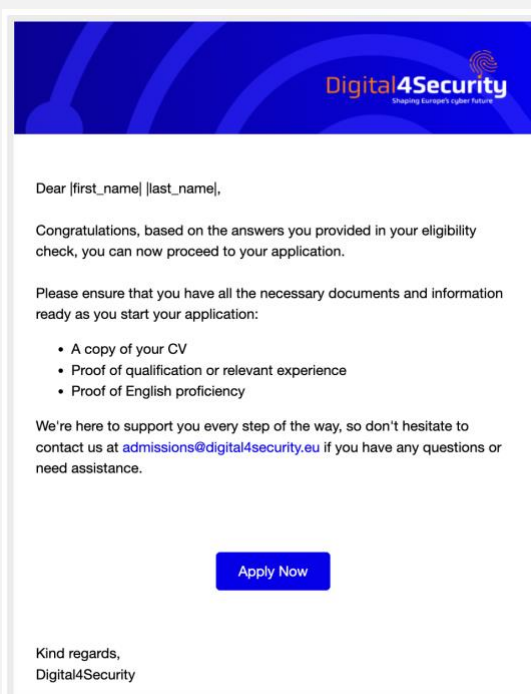


Figure 37: Verification email



## Timeline and milestones



### Key phases of the campaign

(Note: Dates are subject to change depending on accreditation process)

#### **Phase 1: Pre-launch awareness (May 2024 - December 2024)**

**Objective:** Build initial awareness and interest in the Digital4Security Masters Programme.

**Activities:**

- Organic posting on LinkedIn and partner social media channels.
- Attendance and promotion at *20x30: Europe's Advanced Digital Skills Summit*.
- Development and dissemination of informational brochures and prospectuses.
- Setup of detailed module pages on the website with introductory videos.
- Engagement through Digital4Security's and partners' newsletters and social media channels.

#### **Phase 2: Pilot programme promotion (November 2024 - January 2025)**

**Objective:** Test interest and gather feedback for refining recruitment strategies.

**Activities:**

- Social media shares highlighting pilot programme details.
- Newsletter outreach to existing subscribers and partner networks.
- Collection of early interest data to refine messaging and engagement strategies.

### **Phase 3: Recruitment kick-off (February 2025)**

**Objective:** Officially open recruitment for the Digital4Security master's programme.

**Activities:**

- Launch targeted digital marketing campaigns, including social media ads and email marketing blasts.
- Develop interactive content, such as infographics or FAQ posts, addressing common questions about the programme and its benefits.
- Collaborate with partners and stakeholders to feature the programme in their newsletters or blog posts.
- Introduce a dedicated "Ask Us Anything" social media campaign, inviting prospective students to submit questions through comment sections or DMs, with responses shared through posts or stories.

### **Phase 4: Ongoing recruitment and engagement (March 2025 - October 2025)**

**Objective:** Maintain momentum in student recruitment and deepen engagement with potential applicants.

**Activities:**

- Continuation of social media campaigns and email marketing with updated content featuring student testimonials, faculty interviews, and application tips.
- Participation in educational fairs and industry conferences to promote the programme and directly recruit students.

### **Phase 5: Final push and closure of initial recruitment cycle (November 2025 - January 2026)**

**Objective:** Finalise the recruitment for the first cohort.

**Activities:**

- Intensify email reminders about application deadlines.
- Host last-minute Q&A sessions and webinars to address prospective students' queries.
- Review and process applications to meet enrolment targets.

---

## **Milestones for tracking progress**

### **Milestone 1: Launch of campaign website and module pages (June 2024)**

**KPIs to track:**

- Number of visitors to the website.
- Engagement metrics on module pages (e.g., video views, downloads of syllabi).

## **Milestone 2: Pilot programme completion and feedback (January 2025)**

### **KPIs to track:**

- Number of participants in the pilot programme.
- Feedback collected on messaging, accessibility, and programme attractiveness.

## **Milestone 3: Recruitment kick-off launch (February 2025)**

### **KPIs to track:**

- Early application interest and inquiries generated during the first month.
- Social media reach and engagement metrics.

## **Milestone 4: Mid-campaign review (August 2025)**

### **KPIs to track:**

- Number of applications received vs. target.
- Demographic breakdown of applicants.
- Conversion rate from inquiries to applications.

## **Milestone 5: Close of initial recruitment cycle (January 2026)**

### **KPIs to Track:**

- Total number of enrolled students.
- Completion of enrolment goals (e.g., gender balance, geographic diversity).
- Feedback from applicants on the recruitment process.

## **Milestone 6: Post-Campaign Review and Preparation for Next Cycle (February 2026)**

### **KPIs to Track:**

- Analysis of campaign effectiveness.
- Identification of areas for improvement.
- Detailed plan for the next recruitment cycle based on lessons learned

## Monitoring and evaluation



### Metrics and KPIs to measure success

To ensure the effectiveness of the Digital4Security launch campaign, the following key performance indicators (KPIs) will be monitored:

- **Website traffic:** Number of unique visitors and page views on the Digital4Security website.
- **Engagement rates:** Interaction metrics such as video views, downloads of informational materials, and time spent on site.
- **Application numbers:** Total applications received, completion rate of applications, and conversion from register your interest to application.
- **Demographic diversity:** Breakdown of applicant demographics to assess diversity targets.
- **Social media reach and engagement:** Number of followers, post reach, engagement rates (likes, comments, shares), and conversion to website traffic.
- **Newsletter performance:** Subscription rates, open rates, and click-through rates on content links.

### Tools and methods for data collection and analysis

- **Website analytics:** Matoma is used track and analyse website visitor behaviour and engagement.
- **Social media analytics tools:** Platforms like Hootsuite or Buffer to measure engagement and effectiveness of social media campaigns.
- **Moodle LMS platform:** We will work with the academic partners to identify the best analytics plugin to use (e.g. [https://moodle.org/plugins/local\\_learning\\_analytics](https://moodle.org/plugins/local_learning_analytics))
- **Webinar platforms:** The consortium will select the most suitable tool that can provide analytics on attendees.

- **Full Fabric CRM:** To track interactions with potential students from initial contact through to application.
- **Feedback surveys:** Surveys during course and post course completion to gather qualitative feedback from participants and stakeholders.
- **EUSurvey:** Our online survey management system of choice for creating and publishing forms available to the public. As the European Commission's official survey management tool it provides a wide variety of elements from multiple-choice questions to advanced multimedia elements.

## Feedback mechanisms and continuous improvement

**Regular review meetings:** Monthly meetings with the marketing and recruitment teams to review campaign performance against KPIs.

**Stakeholder feedback:** Regular collection of feedback from university partners, industry associations, and directly from students.

**Data based content optimisation:** Continuous testing of different messaging and marketing materials to optimise engagement and effectiveness.

**Adaptation and Iteration:** Quick adaptation of strategies based on analytical insights and stakeholder feedback to improve ongoing and future campaign efforts.

## Risks and mitigation strategies



### Potential challenges and obstacles

- **Lower than expected application rates:** Risk of not meeting application targets due to competition or lack of awareness.
- **Technical issues with digital tools:** Problems with the website, LMS or webinar platforms that could impair user experience and participation.
- **Changes in market demand:** Shifts in the job market, technologies or industry needs that could affect the relevance of the programme content.
- **Potential Challenge: Competition with Similar Programs:** The Digital4Security program may face stiff competition from similar initiatives, which could divert potential applicants and impact enrolment numbers.

### Contingency plans

- **Enhanced marketing efforts:** Increase advertising budget, expand social media campaigns, and partner with influential industry bodies to boost visibility if application rates are low.
- **Technical backup plans:** Establish backup systems and support for all digital platforms to ensure smooth operation during high traffic periods and live events.
- **Curriculum flexibility:** Regular reviews of course content with industry partners to ensure the program remains aligned with current job market demands and technology trends.
- **Crisis management team:** A dedicated team to handle unforeseen events or public relations issues that could impact the program's reputation or recruitment efforts.

## GDPR



The Digital4Security nominated DPO is Costin Carabas.

Currently the project website, Full Fabric and Moodle LMS are hosted on servers within the EU. All data and backups are stored within the EU. Full Fabric and Moodle links to the project Privacy Policy: <https://www.digital4security.eu/privacy-policy/>



#### Legal Disclaimer

The European Commission's support to produce this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

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

Copyright © 2024 by Digital4Security Consortium



# Digital4Security

Shaping Europe's cyber future



Co-funded by  
the European Union