

A.B Institute of Entrepreneurship Development
Cyprus

National Course Plan



Co-funded by
the European Union

Contents

Target group description	3
Training setting	3
Learner Journey(s)	5
Conclusion	8

MECyS is funded by the European Union.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA).

Neither the European Union nor EACEA can be held responsible for them.

Target group description

The target group for the MECyS training in Cyprus consists of employees and managers in Micro and Small Enterprises (MSEs). This group is heterogeneous, with varying levels of education, and knowledge based on their work positions. The MSEs in Cyprus operate across different sectors, adding to the diversity within the target group.

The training will primarily focus on the Beginner (Turtle) and Intermediate (Mouse) levels, given the specific needs of MSEs in the region. These individuals have limited time for self-learning and training due to the competitive nature of their businesses.

The Course Plan is designed to accommodate their time constraints, featuring asynchronous online learning, self-regulated elements, and practical, hands-on content. The aim is to make the training appealing, necessary, and aligned with the digitalization and data protection requirements of MSEs.

Training setting

The MECyS training will be delivered entirely online, providing flexibility for the target group.

The structure remains as follows:

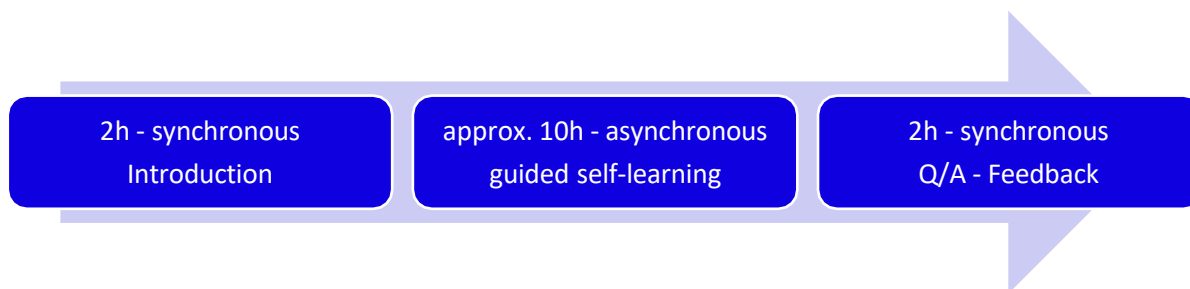
- **4 hours of synchronous learning** (trainer-led)
- **10 hours of asynchronous learning** (self-paced modules)
- **Completion time: 1 month**

Synchronous Sessions Breakdown

- **2 hours - Introduction Session**
 - Orientation to the training platform and tools
 - Assessment of participant backgrounds and cybersecurity knowledge
 - Guidance on navigating the course modules
- **2 hours - Final Q/A and Feedback Session**
 - Evaluation of participant understanding and progress
 - Group discussion on case studies and real-world applications
 - Collection of feedback for course improvement

Asynchronous Learning Modules (10 hours total)

The training includes self-regulated learning through interactive tools, quizzes, and real-life cybersecurity simulations.



Number of Participants

The training is designed to be flexible, targeting 3 to 5 Micro and Small Enterprises (MSEs) and a varying number of university students, with the exact number of participants from each entity remaining adaptable. This approach allows for a tailored experience as part of the pilot phase, utilizing the course developed by AB IED to meet the specific needs and capacities of the participating businesses and students without being able to commit to a fixed participant count at this stage.

Relevant Contents

The training will cover all contents relevant to the Beginner and Intermediate levels, as defined in the Course Plan.

Learning Materials

The training program will incorporate a carefully curated selection of practical materials, including websites, online tools, games, and presentations, to enrich the learning experience. These resources have been chosen for their effectiveness in enhancing cybersecurity knowledge and skills across various learning styles and professional needs. Below is a closer look at some of the key tools that will be used in the course:

ENISA Cybersecurity Maturity Assessment for SMEs: An online tool that provides SMEs with a structured framework to assess their cybersecurity maturity level. It helps identify gaps and offers guidance on strengthening security measures.

AI-Powered Cybersecurity Chatbot: This interactive chatbot provides real-time assistance by answering cybersecurity-related questions, generating personalized explanations, and even offering custom quizzes to reinforce learning.

Virtual Cybersecurity Escape Room (VCSER): A gamified learning experience where participants engage in cybersecurity puzzles and real-world threat scenarios. This tool promotes teamwork and problem-solving while reinforcing core cybersecurity concepts.

GDPR Quiz: An interactive quiz designed to test and improve participants' knowledge of data protection laws, particularly GDPR. It ensures that learners understand the regulatory and compliance aspects of cybersecurity.

Evaluation Quiz: A structured final quiz to assess participant progress, evaluate learning outcomes, and reinforce key cybersecurity principles covered in the training.

These tools integrate interactive simulations, assessments, and strategic guidance, creating a dynamic and comprehensive learning experience. By leveraging these resources, the MECyS training aims to equip Micro and Small Enterprises in Cyprus and university students with practical cybersecurity skills and knowledge, ensuring they are prepared to navigate the challenges of digital security and data protection in today's evolving landscape.

Trainers' Background

The trainers delivering the MECyS course have a background in data protection and cybersecurity, both in terms of education and practical application. They are both members of the IED Group with extensive experience in data protection and cybersecurity applications.

Learner Journey(s)

The learner journey will follow the training methodology outlined for Level 1 & 2 in the overall MECyS Training Plan, adapting it to the specific needs of MSE professionals and university students.

What?

The MECyS training program in Cyprus will provide fundamental knowledge in two key areas:

Fundamentals of Cybersecurity: This section will introduce basic concepts, terminology, and principles of cybersecurity, tailored to the needs of both professionals and students.

Fundamentals of Data Protection: Participants will develop an understanding of data protection principles, regulations, and the importance of safeguarding personal and business data.

How?

The training methodology follows a practical, hands-on approach, leveraging interactive tools and resources to build cybersecurity skills and effective data protection practices.

Practical Cybersecurity Skills: Participants will engage in hands-on exercises using tools such as:

ENISA Cybersecurity Maturity Assessment for SMEs to evaluate and improve security practices.
AI-Powered Cybersecurity Chatbot for real-time cybersecurity guidance, simulated threat analysis, and custom quizzes to reinforce learning.

Virtual Cybersecurity Escape Room (VC SER) for interactive problem-solving in cybersecurity attack scenarios.

Data Protection Implementation: To enhance understanding and application of data protection techniques, participants will engage with:

GDPR Quiz to assess and improve their knowledge of data protection regulations.
Practical exercises and self-assessments to apply cybersecurity principles in business and personal contexts.

Why?

The training emphasizes the real-world relevance of cybersecurity for both MSEs and university students:

Cybersecurity Relevance: Participants will explore real-world case studies demonstrating the impact of cyber threats on businesses and individuals.

Data Protection Importance: The course will illustrate the consequences of data breaches, their impact on organizations and individuals, and how regulatory compliance plays a role in cybersecurity strategies.

When?

The pilot course will be delivered in the first half of 2024, with additional sessions being tested and refined for future course cycles.

MECyS Training Course Outline

Introduction to the Course (Synchronous)

- Welcome and Course Overview
- Objectives and Learning Outcomes
- Introduction to the Training Platform and Tools

Part 1: Fundamentals of Cybersecurity (Asynchronous)

- Cybersecurity Basics: Concepts, Terminology, and Principles
- Understanding Cyber Threats and Vulnerabilities
- Importance of Cybersecurity for MSEs and University Students

Part 2: Practical Cybersecurity Skills (Asynchronous)

- Utilizing ENISA Cybersecurity Maturity Assessment for SMEs to evaluate and enhance security posture
- Engaging with the AI-Powered Cybersecurity Chatbot for real-time cybersecurity guidance and quizzes
- Applying Cybersecurity Best Practices in Business and Academic Environments

Part 3: Fundamentals of Data Protection (Asynchronous)

- Introduction to Data Protection: Principles and Regulations
- The Role of Data Protection in Business and Personal Use
- Implementing Data Protection Strategies in Workplace and Academic Settings

Part 4: Interactive Cybersecurity Learning (Asynchronous)

- Engaging in the Virtual Cybersecurity Escape Room (VCSE) for hands-on security challenges
- Understanding GDPR Compliance through the GDPR Quiz
- Practical Scenario-Based Exercises to reinforce Data Protection knowledge

Part 5: Hands-on Exercises and Case Studies (Asynchronous)

- Self-Guided Scenario Analysis: Participants analyze real-world cybersecurity incidents and apply solutions
- Interactive Quizzes and Challenges: Utilize tools like the AI Chatbot and Escape Room for cybersecurity problem-solving
- Application-Based Learning: Simulated exercises to reinforce cybersecurity awareness and data protection strategies

Evaluation and Feedback (Synchronous)

- Evaluation of participant understanding through the MECyS Platform Final Quiz
- Feedback form for participants to share their learning experiences and provide suggestions

Conclusion (Synchronous)

- Course Wrap-up and Summary of Key Learnings
- Guidance on Continuing Cybersecurity and Data Protection Education

Conclusion

The MECyS Course Plan in Cyprus is designed to meet the specific needs of both Micro and Small Enterprises (MSEs) and university students, focusing on cybersecurity and data protection. Recognizing the challenges of time constraints, digitalization, and evolving security risks, this training program provides a flexible and practical learning experience that equips participants with essential cybersecurity skills.

The content is structured to accommodate different levels of cybersecurity awareness, ensuring

that MSE personnel, staff, management, and students engage in an interactive and participative learning environment. Through real-world case studies, gamified tools, AI-driven learning, and self-assessment activities, participants will develop practical competencies in cybersecurity risk management and data protection strategies.

This finalized English version of the Cypriot National Course Plan ensures alignment with the MECyS partners' objectives, providing a coherent training framework that can be adapted based on local needs. Future refinements will be integrated into the Cypriot version as the training program evolves.



MECyS

Micro - Enterprise Cybersecurity

mecys.eu



Co-funded by
the European Union