

# National training plan

Association of Thessalian Enterprises and  
Industries (STHEV), Greece



Co-funded by  
the European Union

## CONTENTS

1. Summary.....	1
2. Target group description .....	1
3. Training setting .....	2
4. Learner Journey(s).....	3
BEGINNER & INTERMEDIATE (TURTLE & MOUSE) LEARNER JOURNEY .....	3
5. Conclusion.....	4

## 1. Summary

The Greek training prototypes represent a strategic initiative designed to cater specifically to micro and small enterprises. These training programs are meticulously tailored to the unique needs and challenges faced by this target group (TG), aiming to empower them with essential cyber-security knowledge and skills. To achieve this, the training content is carefully adapted to align with the specific requirements of micro and small enterprises, recognizing their distinct context and constraints.

The training initiatives for micro and small enterprises are set to be delivered through online courses, ensuring accessibility and flexibility for business owners and employees. These courses are intended to accommodate a minimum of 60 participants. The curriculum will start from a fundamental level of knowledge of cyber security and data protection providing a strong foundation for participants. At the same time, there will be appropriate training materials for participants who have a deeper knowledge of cyber security and data protection and wish to deepen their knowledge further.

The selection of micro and small enterprises as the target group for these training prototypes is grounded in a comprehensive analysis. The decision is based on insights derived from the "Overview of Vocational Education and Training" (VET), specifically in part 5. Within this overview, there is a notable emphasis on equipping trainees with the necessary tools and skills through various training programs. Additionally, the analysis identifies a significant gap in the training opportunities available for employees working in small and medium-sized enterprises (SMEs).

## 2. Target group description

### **Target Group: Micro and Small Enterprises (MSEs)**

The micro and small enterprises (MSEs) that are the focus of these training prototypes are accessible through STHEV, as they are registered members of this organization. STHEV serves as a valuable conduit to reach these businesses, and it helps ensure that the training initiatives are delivered to the intended audience effectively.

Employees within micro and small enterprises are a diverse group, characterized by a wide range of variables such as age, prior expertise, overall IT experience, levels of motivation and are interested in improving their cybersecurity skills.

Additionally, it's important to acknowledge that employees in these MSEs often have limited time available for seminars and training in the field of cybersecurity. This limitation can be attributed to the demanding nature of their roles within small businesses, where employees often have numerous responsibilities. Recognizing these time constraints is critical when designing training programs, as they must be concise, efficient, and readily accessible to accommodate the busy schedules of MSE employees.

Our target group mainly has minimum or medium-sized experience in cybersecurity and data protection. Given that their positions within MSEs may not be directly tied to cybersecurity responsibilities, it is essential to provide them with foundational knowledge in this domain. The nature of their work positions and the general business context necessitates at least a basic understanding of cybersecurity. Even though they may not be cybersecurity specialists, they need to grasp fundamental principles to protect their businesses from cyber threats and adhere to data protection regulations.

In sum, the training prototypes for micro and small enterprises, accessed through STHEV, are designed to address the unique needs and constraints of this diverse group of employees. These initiatives aim to provide accessible, concise, and tailored training, filling critical knowledge gaps in cybersecurity and data protection. By doing so, they empower employees to better safeguard their businesses in an increasingly digital and interconnected world, ultimately contributing to the overall resilience of MSEs and the broader business landscape.

### 3. Training setting

Given the digital character of cybersecurity, it would be well-suited to conduct MECyS training for the intended audience, i.e., Micro and Small Businesses, in an online setting. To elaborate, this would involve hosting weekly online seminars, potentially in an asynchronous format, with short durations. Alternatively, MECyS training could be either integrated into ongoing events, particularly those related to the MECyS domain, or information sessions for MSEs, where this target group typically participates or is held in an online synchronous way.

The proposed schedule is to have around 6 hours of asynchronous training and 2 hours of synchronous either face-to-face or online training. The total duration will be 1 to 4 weeks and the group size of the target group will be 60 participants with the aim of creating 4 groups of 15 people at least.

Additionally, participants in TG could be reached through members of STHEV, but also through associated partners of STHEV and their network.

For TG-Micro and Small Enterprises, the content ranges from basic to intermediate levels, depending on their specific requirements and existing knowledge. These two groups can be integrated into one since their level of knowledge and needs are very close.

Finally, we will use interactive content such as games, quizzes, exercises, and educational videos.

## 4. Learner Journey(s)

Taking into consideration the level of their knowledge the structure of the training will be as follows:

### BEGINNER & INTERMEDIATE (TURTLE & MOUSE) LEARNER JOURNEY

#### 1. What?

Fundamentals of cybersecurity field: This section provides an initial exploration of core concepts, industry-specific terms, and the critical role of cybersecurity in the context of business operations. It further explores the examination of common attack vectors, including those associated with email, web, and network-based attacks, and covers the fundamental practices and principles for safeguarding data and information.

#### 2. How?

Practical examples: In this section, the focus is on teaching businesses how to assess their specific cybersecurity risks and vulnerabilities, providing guidance for the creation and implementation of security policies tailored to the business's needs, and demonstrating the usage of security tools and technologies such as antivirus software and firewalls.

### 3. Why?

Significance of cybersecurity: In this section, emphasis is placed on the importance of safeguarding sensitive customer and company data, highlighting how a data breach can significantly impact a business's reputation and erode customer trust. Moreover, scenarios, case studies, and interactive games will be integrated to further illustrate these concepts and engage participants in practical learning.

### 4. Me?

Individualized education: In this section, the focus will be on addressing the role of individual employees in maintaining cybersecurity, including their capacity to recognize threats and practice safe online behavior.

## 5. Conclusion

The MECyS training project in Greece targets professional workers in Micro and Small enterprises. It provides online training to cater to the busy schedules of these professionals. The outreach strategies involve forming partnerships and utilizing professional networks through STHEV.

The training content is tailored to the participants' existing knowledge and includes interactive materials. The professional workers pathways are structured based on prototypes from the overall MECyS training plan and cover a progression from basic to intermediate skills in cybersecurity and data protection. By implementing this training prototype, we aim to assess the level of cybersecurity awareness in micro and small enterprises and raise awareness among participants about potential challenges we may encounter in the future.



# MECyS

*Micro - Enterprise Cybersecurity*

[mecys.eu](https://mecys.eu)



Co-funded by  
the European Union