

National Course Plan

School of Business, University of Applied Sciences
and Arts Northwestern Switzerland (FHNW)



Co-funded by
the European Union

CONTENTS

1. Target Group description	3
Target Group 1 (TG1).....	3
Target Group 2 (TG2).....	3
2. Training setting.....	4
Course Delivery	4
Course Duration	4
Learning Format.....	4
Outreach Strategy	4
Training Content and Learning Resources	5
Required Expertise.....	5
3. Learner Journeys.....	6
Beginner & Intermediate (Turtle & Mouse) learner journey.....	6
Advanced (Hare) learning journey	8
4. Conclusion.....	10

This project is financially supported by Movetia (www.movetia.ch). Movetia promotes exchange, mobility and cooperation within the fields of education, training and youth work – in Switzerland, Europe and worldwide. However, this document reflects the views only of the authors, and Movetia cannot be held responsible for any use which may be made of the information contained therein.

This work is licensed under [CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/)



1. Target Group description

Referring to the findings from part 7 of the Overview of Vocational Education and Training, two **Target Groups (TG)** can be distinguished for Switzerland.

TARGET GROUP 1 (TG1)

These are people working in MSEs who are interested in improving their cybersecurity skills. They already have some years of working experience outside of cybersecurity. They might have the motivation to improve their job perspectives by upskilling in the field of digitalization. They might also be motivated as they are in a responsible position in their MSE and need to understand cybersecurity and data protection risks.

From practical experience, this TG is very heterogeneous. People have diverse working experiences and educational backgrounds. Nevertheless, this heterogeneity can be used for a fruitful exchange and lateral learning.

TG1 should be prioritized since they often have less time for training and learning. They may as a result dedicate only about 2 to 3 hours per week. In this regard, they need fast and effective learning tools. MECyS would therefore be beneficial to them by providing such learning tools that meet their learning requirements.

Given that these potential learners are already in MSEs, they already understand to some extent the relevance of cybersecurity and data protection. They are therefore more likely to assimilate the provided learning material.

TARGET GROUP 2 (TG2)

The participants in this TG are students at applied universities – typically they would work part-time. At a minimum, a typical student at FHNW as example, possesses one year of working experience before starting studies. These students may not have enough time to take a complete cybersecurity course during their studies. However, they are likely to choose to enrol in a MECyS training if it is offered as an elective course in their program or if it is linked to their studies in a seamless manner. Alternatively, TG2 may choose to enrol in a MECyS training upon completion of their studies to add to the attractiveness of the curriculum vitae as they prepare to join the labour market.

TG2 is still heterogeneous, however members are typically in similar age groups and possess just initial working experience in rather non-leading positions.

2. Training setting

MECyS training for both TG1 and TG2 could be structured as follows.

COURSE DELIVERY

In line with the digital nature of cybersecurity, the MECyS training for both target groups would ideally be delivered in an online setting. Alternatively, MECyS training could be offered as part of existing events where this TG is typically present (e.g., industry-specific fairs or as add-on to existing well-attended events/courses).

COURSE DURATION

Given the time constraints, a course with flexible, self-paced learning materials could be beneficial. This could range from less than 1 hour (just a learning nugget) up to an estimated maximum a few days (spread across several days/weeks). Also, self-paced courses would be beneficial, so that the learners are able to decide about speed/duration by themselves.

LEARNING FORMAT

The combination of trainer-based and self-regulated learning should be valuable to both groups but in varying proportions. For TG1, due to their pre-knowledge and motivation, a higher proportion of self-regulated learning using online tools, complemented by recorded webinar sessions which they can access at any time, could be more beneficial. For TG2 a combination of online and in-person lectures, practical assessments, and self-regulated learning tools could be made available.

OUTREACH STRATEGY

Participants in TG1 could be reached through direct communication with MSEs, for example partnerships with company. Engagement on professional networking sites and advertisements through startup networks like the Impact Hub Community will also be useful methods to reach participants in TG1. It could also be feasible to reach this TG via personal contacts of TG2 – meaning that students of FHNW could reach TG1 members in their work environment. Moreover, TG1 could be reached via the further education offered by FHNW.

Concerning TG2, applied universities would play a crucial role in reaching out to the participants of the group. Collaborating with educational institution will facilitate the integration of the MECyS training into students' study plan as an elective. TG2 could be reached via the bachelor and master programs offered at FHNW. The deans of the study courses could be approached to reach this group.

TRAINING CONTENT AND LEARNING RESOURCES

Relevant content for both target groups may vary depending on the potential participant's initial knowledge of cyber security. Still, a rough assumption can be made that interactive materials such as games, quizzes, and video tutorials could be beneficial for TG1 and TG2. Specially for TG2, they could also be provided with guiding reading or video materials and practical simulations. It is critical to not overwhelming the participants and to offer a modular approach.

REQUIRED EXPERTISE

The trainer(s) leading the course should have substantial experience in the field of cybersecurity and/or data protection, both in terms of professional experience and in teaching or coaching roles, to effectively facilitate both self-guided and traditional teaching methods. Ideally, they should also be conversant with Switzerland's educational framework, especially when targeting participants in TG2. They should be able to communicate in easy-to-understand language and should have the skill to adapt contents to the practical fields of the participants.

A summary of the course setting is available in the **Table 1** below:

Description	Target Group 1	Target Group 2
Course delivery	Online, offline (as part of events)	Online, offline (as part of events)
Course duration	1 to 4 weeks	4 weeks to 1 semester (4 months max)
Training format	Trainer-based and self-regulated learning	Trainer-based and self-regulated learning

Outreach strategy	-Partnerships with MSEs -LinkedIn -Startup communities	Partnerships with industry associations
Training content and learning resources	Games, quizzes, and video tutorials	-Games, quizzes, and video tutorials -Guiding reading materials -Practical simulations
Required expertise	-Knowledge and experience in cybersecurity -Lecturing and coaching ability	-Knowledge and experience in cybersecurity -Lecturing and coaching ability

As the course can be delivered online, there is a high potential for scalability as well the possible to accommodate a large group of participants, provided that efficient digital infrastructures are in place. Further, an online format poses no constraints to the replicability of the course.

3. Learner Journeys

In Switzerland, we have the special situation that a revised Data Protection Law is in force since September 2023. MSEs are currently still building up their knowledge and are heavily in need for data protection knowledge. Cybersecurity is an essential part of data protection. Hence for Switzerland, we will have a learning journey combining both cybersecurity and data protection.

BEGINNER & INTERMEDIATE (TURTLE & MOUSE) LEARNER JOURNEY

Proposed in the MECyS Overall Training Plan¹ structure with leading questions (What? How? Why? Me?) can be a good fit both for TG1 and TG2 if learners only start exploration of the cybersecurity field or have basic knowledge and want to enhance their knowledge.

¹ <https://mecys.eu/wp-content/uploads/2023/09/Training-Plan-September-2023.pdf>

Turtle & Mouse learning journey for Target Group 1 (TG1): MSE Cybersecurity and Data Protection Baseline-Professional

1. What?

Fundamentals of Cybersecurity: Introduction to basic concepts, terminology, and principles of cybersecurity tailored for MSE professionals.

Fundamentals of Data Protection: Introduction to data protection and the importance of protecting data.

2. How?

Practical Cybersecurity Skills: Hands-on training with interactive tools, simulations, and scenarios. Focus on skills and actions relevant to MSE cybersecurity.

Data Protection Implementation: Data protection principles, legal frameworks and data protection techniques or technologies.

3. Why?

Cybersecurity Relevance: Understanding the significance of cybersecurity in the MSE context. Real-world case studies and scenarios.

Data Protection Relevance and Implications: Consequences of data breaches, impact of data breaches on the company, and case studies of data breaches.

4. Me?

Personal Cybersecurity Role: Encouraging self-reflection and self-positioning of individuals within MSEs regarding cybersecurity. Importance of individual responsibility.

Your Role in Data Protection: Handling personal and sensitive data, recognising and responding to data breaches.

Turtle & Mouse learning journey for Target Group 2 (TG2): Cyber Security & Data Protection Baseline-Explorer

1. What?

Introduction to Cybersecurity: Basic understanding of cybersecurity concepts and their everyday life relevance.

Introduction to data protection: Defining data protection and its relevance in different sectors.

2. How?

Practical Cybersecurity Awareness: Practical examples and exercises to increase awareness and skills related to cybersecurity.

Data Protection Functionality: Overview of data protection laws and regulations, data protection techniques

3. Why?

Cybersecurity Importance: Exploring the significance of cybersecurity knowledge in various professional contexts, including MSEs.

Data Protection Relevance: Case studies of noncompliance with data protection laws and consequences of data breaches.

4. Me?

Personal Cybersecurity Awareness: Encouraging learners to reflect on their role in promoting cybersecurity in their future careers and the MSEs they may work for.

My Role in Data Protection: Personal responsibility; Recognising and responding to data breaches.

ADVANCED (HARE) LEARNING JOURNEY

Five-steps learning journey template provided in the Section 5.2 of Overall Training Plan is relevant for Switzerland as well, because Switzerland is a country with a strong focus on

innovation and digitalization, so the number of people with initial cyber security knowledge probably is high enough to apply this template to TG1 and TG2.

Following steps which will be specified for each TG proposed:

1. Risk Assessment and Evaluation
2. Specialized Training
3. Intermediate Assessment
4. Team Communication and Traini
5. Final Certification and Improvement

Advanced Learning Journey for Target Group 1 (TG1): MSE Cybersecurity and Data Protection Deep-Dive Professional

1. Risk Assessment and Evaluation: Conducting risk assessments specific to the MSE's cybersecurity needs.
2. Specialized Training: Tailored courses based on the results of the risk assessment. Focused on addressing specific cybersecurity gaps.
3. Intermediate Assessment: Evaluating progress and strengthening areas of vulnerability.
4. Team Communication: Developing the ability to communicate cybersecurity concerns and strategies within MSE teams.
5. Final Certification and Improvement: A comprehensive assessment leading to certification for those who excel, followed by guidance on further enhancing cybersecurity knowledge and skills if necessary.

Advanced Learning Journey for Target Group 2 (TG2): MSE Cybersecurity and Data Protection Deep-Dive Explorer

1. Risk Assessment and Evaluation:
 - 1.1. Identifying Cybersecurity Risks: Learn to spot potential cybersecurity risks within MSEs.
 - 1.2. Assessment Tools: Gain skills in using risk assessment tools.
2. Specialized Training:
 - 2.1. Customized Cybersecurity Courses: Based on risk assessments, receive training to address specific cybersecurity gaps.

- 2.2. Advanced Skills: Focus on advanced cybersecurity skills needed in MSEs.
- 3. Intermediate Assessment:
 - 3.1. Progress Check: Evaluate your cybersecurity knowledge and skills improvement.
 - 3.2. Addressing Weaknesses: Identify areas needing further attention.
- 4. Communication and Training: Learn how to convey cybersecurity concerns within MSE teams.
- 5. Final Certification and Improvement (4 weeks):
 - 5.1. Comprehensive Assessment: A final evaluation of your cybersecurity proficiency.
 - 5.2. Certification: Receive certification for outstanding performance.
 - 5.3. Continuous Improvement Plan: Get guidance for ongoing skill enhancement.

4. Conclusion

MECyS Course Plan for Switzerland is designed for two distinct Target Groups: Target Group 1 (MSE professionals) and Target Group 2 (students with limited cybersecurity knowledge). The plan offers flexible online and offline delivery, accommodating busy schedules of both groups. Outreach strategies include partnerships, professional networks and educational institutions.

The training content varies based on prior knowledge of attendees, featuring interactive materials and practical simulations.

Learner journeys that are based on prototypes from the MECyS Overall Training Plan are structured, progressing from fundamentals to advanced skills in fields of cybersecurity and data protection. Thus, this plan is well-suited to equip participants with critical skills and knowledge for the Swiss business landscape.

The finalized English version of the Swiss National Course Plan was to basically align the Course Plans of the MECyS partners. Further developments will be done in the Swiss version.



MECyS

Micro - Enterprise Cybersecurity

mecys.eu



Co-funded by
the European Union