October 2023

CyberSecurity for VET and SMEs

EUROPEAN CYBER SECURITY CURRICULUM

DEVELOPED BY META4 INNOVATIONS E. U.

WORK PACKAGE 3 - EUROPEAN CYBER SECURITY CURRICULUM

Funded by the European Union

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. KA220-VET-C9588303

CONTENTS

ABOUT THE PROJECT

SecureFuture – CyberSecurity for VET and SMEs – is an Erasmus+ project implemented between December 2022 and December 2024. The project is being conducted by a consortium of six partners from five counties, all partners with relevant expertise in vocational education and training (VET) and cybersecurity.

COUNTRY	ORGANISATION
Türkiye	Istanbul Ticaret Universitesi (coordinator)
Türkiye	Istanbul Valiligi
Portugal	Mindshift Talent Advisory
Spain	Media Creativa 2020
Italy	Pragma Engineering
Austria	Meta4 Innovations

The SecureFuture consortium identified that the current training provided at VET schools in the European Union (EU) does not live up to the needs of labour market or that there are countries without training on cybersecurity at this level. Besides, many short and medium-sized enterprises (SMEs) do not have qualified employees among their staff to protect their companies against cyber threats, and finding external assistance on cybersecurity is very costly.

Considering these aspects, the project is developing a European framework, curriculum and training content on cybersecurity to guide VET systems and SMEs who want to equip their students and employees with cybersecurity competences. This document refers to the European Cyber Security Curriculum.

SYNOPSIS

The proposed European Cyber Security Curriculum is the final output of the project's work package 3: WP3 – European Cyber Security Curriculum.

The WP3 leader – Meta4 Innovations e. U. – prepared a work plan, guidelines and templates for all partners to facilitate the design and development of a proposed European Cyber Security Curriculum. As an interconnected development process, this European Cyber Security Curriculum is shaped by the Framework through comparison of current national competencies on cyber security, which was collectively developed by all partners.

A survey across Europe was carried out in all partner countries – Austria, Italy, Portugal, Spain and Turkey – during the month of July 2023, in which a pool of 66 experts provided their inputs, to provide an overview of the respective national needs regarding the curriculum for the project. These inputs were summarised by Meta4 and shared with the partners to concurr the Learning Units of this European Cyber Security Curriculum.

1. CURRICULUM

OVERVIEW

Considering the heterogeneous use of ECVET in partner countries, the average ECVET points per hour of training, the partnership of SecureFuture project agreed as follows:

20 hours of training = 1 ECVET point

The European Cyber Security Curriculum contains 10 modules with a span of 120 hours, which corresponds to 6 ECVET points.

Unit 1: Introduction to Cybersecurity Defense

Introduction

The 'Introduction to Cybersecurity Defense' module is a foundational exploration of cybersecurity for SMEs. It provides a comprehensive understanding of core concepts and principles crucial for safeguarding digital systems and data in the face of ever-changing threats. This module equips learners with the essential knowledge and skills needed to defend against cybersecurity threats and protect critical information assets in today's dynamic landscape.

Objective

The objective is to equip trainees with a solid understanding of core cybersecurity concepts and principles to effectively identify, mitigate, and respond to cyber threats.

LEARNING OUTCOMES

Knowledge	K1. Understand the basic principles of cybersecurity and data protection. K2. Identify common cyber threats and vulnerabilities. K3. Comprehend the legal and ethical aspects of cybersecurity.	**Skills**	S1. Demonstrate the ability to analyze network traffic for suspicious activities. S2. Ability to configure firewalls against threats and vulnerabilities. S3. Proficiency in conducting security tests and assessments.	**Responsibility and Autonomy**	RA1. Assess and prioritize security risks to develop a tailored action plan for cybersecurity. RA2. Respond effectively to common cyber threats such as malware or phishing. RA3. Colaborates procedures to minimize the impact of security incidents.

Duration

Contact hours	Hands-on hours	Self-study hours	Assessment hours	TOTAL
0,5	2	9	0,5	12

Unit 2: Data Protection and Privacy

Introduction

This module equips learners with essential competencies for data safeguarding in the digital age. It covers key aspects of data protection, including data classification, responsible handling of sensitive information, privacy, intellectual property, and the complexities of cyber warfare. GDPR and other data protection regulations are emphasized, along with effective data encryption, secure storage practices, and incident response for data breaches. The module fosters attitudes that prioritize privacy, ethics, and adaptability in cybersecurity, enabling learners to actively contribute to digital defense and become vigilant data and privacy protectors.

Objective

To empower learners with the knowledge, skills, and attitudes necessary to effectively protect and manage data, ensuring compliance with data protection regulations and safeguarding privacy in cybersecurity.

LEARNING OUTCOMES

Knowledge	K1. Define data related concepts, including sensitive information, intellectual property and cyber warfare K2. Differentiate data protection regulations related to personal data, digital data, and the General Data Protection Regulation (GDPR) K3. Explain the importance of fostering a mindset that prioritises responsible data handling	**Skills**	S1. Relate adequate encryption techniques to different types of data S2. Apply secure data storage best practices, including encryption, access controls, and regular backups S3. Create data breach management plans considering the severity of breaches	**Responsibility and Autonomy**	RA1. Raise awareness towards safeguarding data and respecting individual privacy rights RA2. Adopt an ethical approach to data handling and intellectual property RA3. Develop a resilient and adaptive attitude towards the ever-evolving cybersecurity threats and regulations

Duration

Contact hours	Hands-on hours	Self-study hours	Assessment hours	TOTAL
0,5	2	9	0,5	12

Unit 3: Risk Management and Compliance

Introduction

This module imparts essential competencies for managing cybersecurity risks and ensuring compliance. It integrates cyber risk management into enterprise-wide risk management practices, acknowledging that complete risk elimination is unattainable. Instead, it focuses on reducing threat impacts through effective cyber risk management programs. The module introduces learners to internationally recognized standards, particularly Information Security Management System (ISMS), outlining key steps and checklists for compliance. In addition to knowledge and skills, the module underscores the development of attitudes related to applying ISMS compliance schemes and recommendations in risk analysis, recognition, and mitigation, empowering learners to proactively address and manage cybersecurity threats fostering a systemic approach to information security.

Objective

To empower learners with the knowledge, skills, and attitudes necessary to effectively apply risk management methodologies also referred to international compliance rules for cybersecurity.

LEARNING OUTCOMES

Knowledge	K1. Define components and requirements of Information Security Management System K2. Identify Information Risk Management as function of Information Security Management System K3. Describe approach to Cybersecurity compliance rules	**Skills**	S1. Identify main components of Information Security Management System S2. Design Risk Management schemes applied to SMEs S3. Examine Cybersecurity compliance rules requirements	**Responsibility and Autonomy**	RA 1. Collaborate in defining Information Security Management System of SMEs RA2. Comply with the Risk Management process RA3. Deal with the adoption of Cybersecurity compliance rules

Duration

Contact hours	Hands-on hours	Self-study hours	Assessment hours	TOTAL
0,5	2	9	0,5	12

Unit 4: Social Engineering and Phishing Awareness

Introduction

This learning unit focuses on social engineering and phishing awareness, vital in our digitally connected world. These topics are as critical as the transformative impact of cloud systems on businesses. By the unit's end, learners will define social engineering, comprehend its motivations (like financial gain and data theft), and recognize various phishing techniques and attack vectors used by cybercriminals. This enhances their threat detection and response capabilities. Learners will also grasp the legal and ethical implications of social engineering attacks, promoting responsible cybersecurity practices. The unit instils ethical awareness, fosters collaboration in incident response, and emphasizes legal compliance. It empowers IT professionals, business owners, VET students, or anyone interested in bolstering cybersecurity knowledge for a secure digital future with confidence and integrity.

Objective

This learning unit aims to equip participants with the knowledge, skills, and ethical attitudes to define social engineering, identify phishing techniques, and understand their legal and ethical implications effectively.

LEARNING OUTCOMES

Knowledge	K1. Define Social Engineering and Its Motivations in the context of SMEs K2. Identify Phishing Techniques and Attack Vectors that make SMEs vulnerable K3. Recall Legal and Ethical Implications of Social Engineering in the context of SMEs	**Skills**	S1. Describe the primary motivations driving social engineering attacks S2. Recognize methods such as spear phishing, vishing (voice phishing), and pretexting S3. Understand the potential consequences for both perpetrators and victims	**Responsibility and Autonomy**	RA1. Promote ethical awareness when defining social engineering motives for responsible, principled use of knowledge. RA2. Collaborate with teams to mitigate phishing threats when identifying attack techniques and vectors. RA3. Independently comply with laws, ensuring legality in social engineering actions and practices.

Duration

Contact hours	Hands-on hours	Self-study hours	Assessment hours	TOTAL
0,5	2	9	0,5	12

Unit 5: Cloud Security for SMEs

Introduction

This unit focuses on addressing the unique security challenges that cloud systems present for SMEs, which increasingly rely on these systems for flexibility, scalability, and cost-efficiency. It is designed to provide SMEs with the knowledge and skills necessary to effectively manage cloud security. The unit is tailored to the specific needs and constraints of SMEs, offering practical insights and actionable strategies to mitigate risks, protect sensitive information, and ensure compliance with industry regulations. Learners will explore core principles of cloud security, cutting-edge technologies, and gain hands-on experience in implementing security measures. Whether a business owner, IT professional, VET student, or someone looking to enhance their cloud security knowledge, this curriculum equips learners with the tools needed to secure their SME's digital future effectively.

Objective

This unit aims to allow learners to have insight into the advantages, possible risks and instructions to maximize the impact of using cloud systems for a SME.

LEARNING OUTCOMES

Knowledge	K1. Identify benefits of using cloud systems for a SME K2. Describe and mitigate the possible risks on using cloud systems. K3. Outlines the preventative steps that might be considered for SMEs' cloud computing security.	**Skills**	S1. Analyse on which aspect and how Cloud computing can be used by SMEs S2. Present security-related queries in a risk management context and propose solutions. S3. Illustrate different types of legal requirements which could have an impact on using cloud systems	**Responsibility and Autonomy**	RA1. Ensure a cloud security in compliance with EU personal data and national protection legislation RA2. Collaborate with colleagues to provide an example scenario on having a Cloud system RA3. Lead a team for assessing security opportunities in a procurement

Duration

Contact hours	Hands-on hours	Self-study hours	Assessment hours	TOTAL
0,5	2	9	0,5	12

Unit 6: Network Security Fundamentals

Introduction

Network security is a crucial concern for SMEs looking to defend against cyber threats. It involves a holistic approach, incorporating physical and software-based safeguards, requiring organization-wide understanding. Learners will gain in-depth knowledge of precautions, encompassing conceptual comprehension and interpersonal skills. They'll learn about available measures for SMEs to manage network security, including forming dedicated teams capable of executing protective actions. This unit empowers participants with the expertise to navigate the intricate field of network security, ensuring they can protect their companies and operations from the evolving landscape of cyber threats effectively.

Objective

This unit aims to provide learners a foundational understanding of network security for SMEs and how to guide their business towards SMEs security.

LEARNING OUTCOMES

Knowledge	K1. Explains the basics terms and concepts of network security K2. Recalls the basic topologies and strategies used in network communication K3. Identifies physical network connection elements and physical security procedures	**Skills**	S1. Discusses why network security is important for an SME S2. Illustrate possible risks and possible solutions in network security S3. Outlines potential network threats and how a SME should react and prevent them.	**Responsibility and Autonomy**	RA1. Leads a constituted team for network security RA2. Provides recommendations on how a company can integrate network security into its business plan RA3. Verify and monitor the implementation of network security procedures

Duration

Contact hours	Hands-on hours	Self-study hours	Assessment hours	TOTAL
0,5	2	9	0,5	12

Unit 7: Secure Software Development

Introduction

Secure software development is paramount in the face of increasing cyber threats. It necessitates embedding security practices across the entire software development cycle, from design and coding to testing, deployment, and maintenance. Its objective is safeguarding data, preserving user privacy, and ensuring software system integrity and availability. Key principles encompass defense in depth with multiple security layers, least privilege for minimal access, and secure-by-design from the project's inception. Regular testing, including penetration testing and code reviews, is essential. Secure deployment, maintenance, and incident response are crucial for ongoing security. Training and awareness, along with supportive resources, further enhance organizational security. Secure software development is indispensable in today's threat landscape, mitigating risks and preserving user trust.

Objective

Learn to implement secure software development practices, safeguarding systems, sensitive data, and user privacy, while minimizing breach and cyber attack risks, and ensuring maintenance, testing, and training.

LEARNING OUTCOMES

Knowledge	K1. Define secure coding practices, common security threats and security standards and frameworks K2. Learn secure development lifecycle and configuration management, secure deployment and maintenance K3. Determine Vulnerability assessment and penetration testing, encryption and cryptography, secure APIs and integrations	**Skills**	S1. Experiment secure coding, vulnerability assessment, security testing, encryption and cryptography S2. Construct secure configuration management, deployment and maintenance, secure API design S3. Improve compliance and privacy regulations, continuous learning	**Responsibility and Autonomy**	RA1. Take notice developers have a responsibility to prioritize security in their coding practices. RA2. Takes decisions on security-related issues during the software development process. RA3. Collaborate with security experts during the development process to ensure that security requirements are properly met.

Duration

Contact hours	Hands-on hours	Self-study hours	Assessment hours	TOTAL
0,5	2	9	0,5	12

Unit 8: Secure Endpoint Protection

Introduction

In today's interconnected world, protecting endpoints, including laptops, desktops, mobile devices, and servers, from cyberattacks is essential. Secure endpoint protection entails implementing a multi-layered defense strategy to shield these devices from malware, ransomware, phishing, and unauthorized access. This involves deploying robust antivirus and anti-malware software, leveraging advanced threat detection and prevention mechanisms, enforcing stringent access controls and authentication measures, and regularly updating software and operating systems. Secure endpoint protection is critical for organizations of all sizes and industries, as it averts data breaches, prevents unauthorized access to sensitive information, and safeguards business continuity. By fortifying endpoints, organizations can reduce the risk of cyberattacks, adhere to industry regulations, and protect their reputation and customer trust.

Objective

Learn to secure laptops, desktops, mobile devices, and servers against malware, ransomware, phishing, and unauthorized access, reducing data breaches and operational disruptions while ensuring compliance and preserving trust.

LEARNING OUTCOMES

Knowledge	K1. Understand endpoint security and an overview of secure endpoint protection Measures K2. Defines Key components of secure endpoint protection, Antivirus, Firewall, and Encryption K3. Determine best practices for Implementing secure endpoint protection, patch management, threat detection, and user training	**Skills**	S1. Able to analyze and respond to malware, ransomware, and phishing threats for effective mitigation. S2. Manage and configure endpoint security tools (antivirus, firewalls, encryption) for effective deployment and operation. S3. Capable to patch management, access controls, data encryption, user awareness for endpoint security.	**Responsibility and Autonomy**	RA 1. Secure endpoints with antivirus, firewalls, encryption to counter threats and vulnerabilities effectively. RA2. Assume endpoint security responsibility, identifying, mitigating risks, conducting assessments, and maintaining security. RA3. Swiftly respond to security incidents, investigate, conduct forensics, implement remediation, prevent recurrences.

Duration

Contact hours	Hands-on hours	Self-study hours	Assessment hours	TOTAL
0,5	2	9	0,5	12

Unit 9: Incident Management and Response

Introduction

Incident Management and Response is essential for mitigating a broad range of disruptions and threats. Its purpose is to efficiently identify, analyze, and respond to incidents that can disrupt operations or harm an organization's assets, reputation, and stakeholders. These incidents encompass cyberattacks, data breaches, natural disasters, accidents, and public health emergencies. The main goal is to minimize impact, restore operations, and prevent future incidents, following a structured framework. Successful incident management also demands clear communication and collaboration among teams and stakeholders. A robust strategy enables organizations to proactively address risks, enhance resilience, reduce downtime, protect data, comply with regulations, and safeguard their reputation.

Objective

Learn to respond effectively to minimize incident impact, including prompt detection, resource mobilization, coordinated response, and rapid restoration of normal operations for overall stability and security.

LEARNING OUTCOMES

Knowledge	K1. K1. Make ready Incident Detection and Reporting, Incident Assessment and Analysis K2. Incident Response Planning and Preparedness, Incident Containment and Mitigation K3. To organise Incident Communication and Coordination, Incident Recovery and Lessons Learned.	**Skills**	S1. Analyze incidents, identify causes, and select appropriate response strategies using strong problem-solving skills. S2. Communicate effectively for incident management and response. S3. Apply technical knowledge for incident detection in effective incident management and response.	**Responsibility and Autonomy**	RA1. Prepared for promptly identifying and triaging incidents that occur within an organization. RA2. Assume responsibility for coordinating and executing the response to incidents. RA3. Take charge for documenting and reporting incidents

Duration

Contact hours	Hands-on hours	Self-study hours	Assessment hours	TOTAL
0,5	2	9	0,5	12

Unit 10: Business Continuity and Disaster Recovery

Introduction

Business Continuity and Disaster Recovery (BCDR) are integral to an organization's risk management strategy, ensuring the continuity of critical business operations and the recovery of systems and data in times of disruption. Business Continuity involves proactive planning, identifying vital processes, assessing risks, and developing strategies to maintain business operations during and after a disruption. Disaster Recovery focuses on technical aspects, involving backup and recovery plans, resilient IT systems, and procedures to restore normal operations quickly. Both BCDR elements demand a thorough understanding of an organization's assets, dependencies, and risks. Collaboration and coordination across departments, role clarity, communication, training, and testing are vital. Effective BCDR plans minimize disruption impact, maintain trust, and ensure long-term operational resilience.

Objective

Learn to secure critical business operations, minimize disruption impact, identify risks, develop and test plans to enhance organizational resilience and to ensure long-term viability.

LEARNING OUTCOMES

Knowledge	K1. Define risk Assessment and Business Impact Analysis, Business Continuity Planning K2. Identify to key elements of IT Disaster Recovery Planning and Crisis Management K3. Awareness about Backup and Recovery Strategies relevant for continuity of business operations.	**Skills**	S1. Able to conduct risk assessments and analysis to identify potential threats and vulnerabilities to critical business operations. S2. Create comprehensive business continuity and disaster recovery plans. S3. List procedures, and resources needed to ensure the continuity of critical operations and the timely recovery of systems and data.	**Responsibility and Autonomy**	RA 1. Responsibility for identifying and assessing potential risks and vulnerabilities to critical business operations and IT systems. RA2. Prepared for implementing comprehensive business continuity and disaster recovery plans. RA3. Regularly monitor and test business continuity and disaster recovery plans to ensure their effectiveness

Duration

Contact hours	Hands-on hours	Self-study hours	Assessment hours	TOTAL
0,5	2	9	0,5	12

2. FINAL REMARKS

The European Cyber Security Curriculum developed under the Erasmus+ project SecureFuture was precisely drafted with the inputs provided by the project partners following the national consultations with 66 professionals in the domain of Cybersecurity in their countries.

It takes into consideration the following parameters:

- A modular allocation of training content into ten areas as units of competence and related contents;
- A set of knowledge, skills, responsibility and autonomy compiled in a table for each of the ten learning units;
- Assignment of 6,0 ECVET points to the set of 10 units corresponding to 120 hours of training.

This Curriculum shall serve as the foundation for the development of the European Cyber Security Training Content, as defined in the WP4 – SecureFuture Training Content.

Together, the European Qualifications Framework, the Training Curriculum and Training Content are an innovative value proposition with strong potential to meet European countries' needs regarding training in cybersecurity for VET students and employees of SMEs – the main target groups of the project – and thus prepare well-trained cybersecurity professionals to defend European SMEs from cyber threats.