Curriculum for Cyber Security in SME

A part of the ISALIP Seeding Materials

Co-funded by the European Union

Co-funded by the European Union

ISALIP

This document was produced as part of the Erasmus+ project.

"Information Security Awareness, Literacy and Privacy – ISALIP"

Project Partners:

Betriebswirtschaftliches Forschungszentrum für Fragen der mittelständischen Wirtschaft e. V. an der Universität Bayreuth
(Business Research Center for Small and Medium-Sized Enterprises e. V. at the University of Bayreuth),
Germany
https://www.bfm-bayreuth.de

eCampus-Lausitz e. V.,
Germany
https://www.ecampus-lausitz.de

MYKOLO ROMERIO UNIVERSITETAS,
Lithuania
https://www.mruni.eu

This document was produced as part of the ERASMUS+ project "Information Security Awareness, Literacy and Privacy – ISALIP", Project ID: 2021-2-DE02-KA210-ADU-000051308

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.

1 Introduction

This output document was developed in the ERASMUS+ project ISALIP (“Information Security Awareness, Literacy and Privacy”) as part of the ISALIP Seeding Materials and is intended to give a practical tool for SME in the field of information security.

The “Curriculum for Cyber Security in SME” presents a basis for knowledge transfer in the field of information security. It is based on the "European Credit System for Vocational Education and Training, ECVET" and covers a four-year training plan for employees. The learning modules are linked with ECVET Credits and required skills.

Cyber security is defined here as part of information security. Information security comprises physical security (analogue information), IT security (digital information) and cyber security (threats in cyberspace).

Content Table:

In this way the curriculum includes all relevant topics in the field of cybersecurity and is a draft for comprehensive teaching material which forms a basis for discussion.

The developed curriculum is planned to be revised and elaborated in further projects.

2 Curriculum for Information Security in SME

2.1 Overview

Topics	Training per Year				ECVET Credits
	Year 1	Year 2	Year 3	Year 4	
Year 1: Introduction to Cybersecurity					55
Introduction to Cybersecurity	1				10
Computer and Network Fundamentals	1				15
Information Security Foundations	1				10
Cryptography	1				10
Security Policies and Compliance	1				10
Year 2: Network Security and Ethical Hacking					60
Network Security		1			15
Ethical Hacking and Penetration Testing		1			15
Secure Coding		1			10
Security Tools and Technologies		1			10
Cybersecurity Laws and Ethics		1			10
Year 3: Advanced Topics and Specializations					65
Advanced Cybersecurity Threats			1		15
Cloud Security			1		10
IoT Security			1		10
Cybersecurity Management			1		10
Capstone Project			1		20
Year 4: Elective and Specializations					20+
Elective Courses				1	Varies
Internship/Work Experience				1	Varies
Career Development				1	10
Continuing Education and Certification				1	5
Ethical Hacking and Capture the Flag (CFT) Competitions				1	5

2.2 Year 1: Introduction to Cybersecurity

Introduction to Cybersecurity

Covered topics are the overview of cybersecurity concepts, terminology, and the importance of cybersecurity in today's world. The learning outcome is the understanding of the fundamentals of cybersecurity.

Computer and Network Fundamentals

Covered topics are understanding computer hardware, software, and network basics and introduction to operating systems and network protocols. The learning outcome is to demonstrate knowledge of computer hardware, software and networks.

Information Security Foundations

Covered topics are principles of information security, confidentiality, integrity, and availability (CIA triad) and risk management and threat assessment. The learning outcome is to apply principles of information security and risk management.

Required skills are risk assessment and security policy development.

Cryptography

Covered topics are risk management and threat assessment and cryptographic algorithms and their applications. The learning outcome is to comprehend cryptographic principles and algorithms.

Required skills are encryption and decryption techniques.

Security Policies and Compliance

Covered topics are developing security policies and procedures and understanding compliance frameworks (e.g., GDPR, HIPAA). The learning outcome is the development of security policies and understanding compliance frameworks.

Required skills are policy development and compliance awareness.

2.3 Year 2: Network Security and Ethical Hacking

Network Security

Covered topics are network architecture and design and firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). The learning outcome is to design secure networks and implement security measures.

Required skills are firewall configuration and intrusion detection.

Ethical Hacking and Penetration Testing

Covered topics are introduction to ethical hacking, conducting penetration tests and vulnerability assessments and reporting and remediation. The learning outcome is to conduct ethical hacking assessments and report vulnerabilities.

Required skills are penetration testing and vulnerability analysis.

Secure Coding

Covered topics are writing secure code to prevent common vulnerabilities and best practices for secure software development. The learning outcome is to develop secure code to prevent vulnerabilities.

Required skills are writing secure code and code review.

Security Tools and Technologies

Covered topics are introduction to security tools such as Wireshark, Nmap, and Snort and using security tools for analysis and monitoring. The learning outcome is to utilize security tools for analysis and monitoring.

Required skills are network analysis and tool proficiency.

Cybersecurity Laws and Ethics

Covered topics are legal and ethical considerations in cybersecurity and privacy laws and regulations. The learning outcome is to understand legal and ethical considerations.

Required skills are compliance and ethical behavior.

2.4 Year 3: Advanced Topics and Specializations

Advanced Cybersecurity Threats

Covered topics are in-depth analysis of advanced threats, including APTs and zero-day exploits and incident response and recovery. The learning outcome is to analyze and respond to advanced threats.

Required skills are incident response and threat analysis.

Cloud Security

Covered topics are security considerations in cloud computing and implementing secure cloud environments. The learning outcome is to implement security in cloud environments.

Required skills are Cloud security configuration.

IoT Security

Covered topics are security challenges in the Internet of Things (IoT) and securing IoT devices and networks. The learning outcome is to secure IoT devices and networks.

Required skills are IoT security measures.

Cybersecurity Management

Covered topics are cybersecurity governance and risk management and security awareness and training programs. The learning outcome is to govern and manage cybersecurity.

Required skills are governance and risk management.

Capstone Project

Covered topics are a practical, real-world cybersecurity project or research and Presentation and documentation of project outcomes. The learning outcome is to apply knowledge to real-world projects.

Required skills are practical application and project management.

2.5 Year 4: Elective and Specializations

Elective Courses

Covered topics depend on course. The learning outcome is to specialize in chosen cybersecurity areas.

Required skills are specialized knowledge.

Internship/Work Experience

The learning outcome is to gain practical experience.

Required skills are practical application and real-world experience.

Career Development

The learning outcome is to prepare for a career in cybersecurity.

Required skills are career readiness.

Continuing Education and Certification

The learning outcome is to pursue industry-recognized certifications.

Required skills are certification preparation.

Ethical Hacking and Capture the Flag (CTF) Competitions

The learning outcome is to apply skills in competitive environments.

Required skills are practical challenges and teamwork.

We thank the co-authors from:

BF/M-Bayreuth

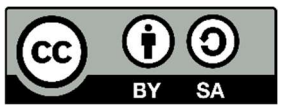
eCampus-Lausitz

Mykolas Romeris University

Information Security Awareness, Literacy and Privacy - ISALIP

Co-funded by the European Union

Co-funded by
the European Union



ISALIP