Module Specification

Cyber Security and Data Protection [TSI]

Version: 2023-24, v2.0, 06 Dec 2023

Contents

Part 1: Information

Module title: Cyber Security and Data Protection [TSI]

Module code: UFCE91-12-M

Level: Level 7

For implementation from: 2023-24

UWE credit rating: 12

ECTS credit rating: 6

College: College of Arts, Technology and Environment

School: CATE School of Computing and Creative Technologies

Partner institutions: Transport and Telecommunication Institute

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: Aims to provide students with an understanding of the duties, roles and responsibilities of professionals within the cybersecurity and data protection industries.

Features: Not applicable

Educational aims: To provide students with an understanding of the role and principles of cybersecurity and data protection, as well as related technologies, tools, legal regulations and standards.

Outline syllabus: Basic concepts and terminology of cybersecurity. Cybersecurity domains. Common Threats
Models of information security. Confidentiality, integrity and availability. Data states. Cybersecurity countermeasures. Security policy.
IT Security management framework.
Cybersecurity Threats, vulnerabilities and attacks. Tactics, techniques and procedures used by cyber criminals.
Technologies and procedures for data integrity providing. Concepts of hashing, digital signatures and digital certificates.
Technologies and procedures for services availability and business continuity. Concepts of high availability.
Technologies and procedures for data integrity providing. Concepts of hashing, digital signatures and digital certificates.
Cybersecurity domains and methods of security audit.
Legislation and legislative responsibility in the field of information security. Personal data: GPDR regulation.

Part 3: Teaching and learning methods

Teaching and learning methods: Learning and teaching will be provided to students in two forms: lectures and practical classes. During lectures, theoretical aspects of the course will be provided to students by the teaching staff. Lectures will be supported by presentation published and available to the students on e.tsi.lv under the module section. The module is based on CISCO materials and will intensively utilise materials of the Cisco Networking Academy.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Identify traits of cybercriminals and security experts, core data protection principles, cybercriminal methods, infosec policies and standards, and data protection laws.

MO2 Use relevant technologies, products and procedures to protect data confidentiality; ensure data integrity and provide data high availability.

MO3 Apply standards and frameworks associated with data protection and cybersecurity.

Hours to be allocated: 120

Contact hours:

Independent study/self-guided study = 112 hours

Face-to-face learning = 48 hours

Total = 160

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://rl.talis.com/3/uwe/lists/D3F267FC-0C96-C0A8-3835-4A8D2862BCB3.html?lang=en-gb&login=1

Part 4: Assessment

Assessment strategy: The module consists of 2 assessments:

Examination for 2 hours. The examination will contain theoretical questions and practical tasks.

Portfolio (practical assignment) During module students should develop and complete individual works. The practical classes are adopted from CISCO Networking Academy, from the course dedicated to the cybersecurity. All items are subject of individual completion.

The resit will be similar to the main sit.

Assessment tasks:

Portfolio (First Sit)
Description: Series of practical assignments.
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested: MO2, MO3

Examination (First Sit)
Description: Exam (2 hours)
Weighting: 50 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1

Portfolio (Resit)
Description: Resit relevant labs from the ones sat at the first sit.
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested: MO2, MO3

Examination (Resit)
Description: Exam (2 hours)
Weighting: 50 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Computer Science (Data Analytics and Artificial Intelligence) {Double Degree} [TSI] MSc 2023-24