

Professional Master's degree program "Cybersecurity Management"

Study Course Title	Security policy, legal and ethical aspects
Study Course Code	SDSKM019
Branch of Science	Cross-sectoral, Business management, Law
Credits (ECTS)	6
Total Number of Contact Hours	48
Number of Lecture Hours	12
Number of Seminar and Practical Assignment Hours	36
Number of Hours for Laboratory Assignments	0
Independent Study Hours	102
Language of Instruction	Latvian and English
Course Approval Date	15.01.2026
Responsible Unit	BA School of Business and Finance of the University of Latvia

Study form	Lectures	Seminars and Practical Assignments	Laboratory Assignments	Independent Studies
Full-time Regular Studies	12	36	0	102
Distance learning	2	10	0	138

Course Developer

First Level Professional Higher Education Program, lecturer Gatis Polis

Prerequisite Knowledge

Prerequisite knowledge required for the acquisition of the course corresponds to the study programme admission requirements and the general knowledge, skills and competences obtained at the previous level of education.

Study Course Abstract

The course provides knowledge about regulatory acts governing privacy, data protection, e-services, and information security. It offers an understanding of information security policy and the fundamental principles of its development. The course gives insight into legal violations and the investigative processes related to information security. It introduces preventive measures for ensuring information security and data protection. Students learn about information security management standards.

The aim of the course is to enhance students' understanding and knowledge of ICT development trends and the legal framework in the fields of cybersecurity, information security, and data protection.

Course Plan Full-time Regular Studies

1. Legal Framework Regulating Privacy, Data Protection, Electronic Services, and Information Security 4L
 2. Security Breaches and Legal Investigation in the Context of Information Security 4S 8Pd
 3. Information Security Policy and Its Core Development Principles 4L 2S 4Pd
 4. Information Security Governance Standards and Best Practice Guidelines 4L 2S 4Pd
 5. Preventive Actions to Ensure Data Protection 4S 8Pd
- Total 12L 12S 24Pd

Course Plan Distance learning

- 1. Legal Framework Regulating Privacy, Data Protection, Electronic Services, and Information Security 2L 2S
 - 2. Security Breaches and Legal Investigation in the Context of Information Security 2S
 - 3. Information Security Policy and Its Core Development Principles 2Pd
 - 4. Information Security Governance Standards and Best Practice Guidelines 2Pd
 - 5. Preventive Actions to Ensure Data Protection 2Pd
- Total 2L 4S 6Pd

Characterization of students' independent work organization and tasks

Students prepare for discussions, participate in seminars and case analysis discussions, develop and present practical individual and group assignments, and prepare for the exam.

Learning Outcomes

Knowledge:

- 1. Demonstrates knowledge and understanding of information security management issues and their influence on an organization's competitiveness, development, and stable, sustainable operations.

Skills:

- 2. Is able to independently identify and critically analyse cybersecurity-related risks, define, plan, and monitor the outcomes needed for risk mitigation.
- 3. Can develop and implement innovations and improvements at the operational, tactical, and strategic levels of cybersecurity management.

Competence:

- 4. Demonstrates the ability to collaborate and communicate effectively, providing consultation, explanation, and justification of information security management goals and results to both expert and non-expert stakeholders.

Requirements for Awarding Credits

Interim Assessments:

- 1. Classroom discussions and practical assignments – 20% of the final grade
- 2. Group work in class – 25% of the final grade
- 3. Individual project development and presentation – 40% of the final grade

Final Examination:

- 4. Exam. Weight in the total evaluation: 15%.

The assessment is graded on a 10-point scale.

Criteria for Evaluating Learning Outcomes

In accordance with Regulations of the Cabinet of Ministers of the Republic of Latvia, at the end of the course, students' knowledge is evaluated according to the following criteria: the amount and the quality of the obtained knowledge, acquired skills and competence in compliance with the planned learning outcomes.

Type of Assessment	Learning Outcomes			
	1	2	3	4
1. Discussions	+	+	+	+
2. Practical work in the classroom	-	+	+	+
3. Independent work and presentation	+	+	-	+
4. Written exam	+	+	+	+

Compulsory Reading List

Edgar T.W., Manz D.O. Research methods for cyber security, Elsevier, 2017

Further Reading List

Privacy and Cybersecurity resources by ISACA:

<http://www.symantec.com/products-solutions/training/theme.jsp?themeid=ssap>

http://csrc.nist.gov/organizations/fissea/2009-conference/presentations/fissea09-mgupta-day3-panel_process-program-build-effective-training.pdf

Plagiarism and other academic misconducts are not permitted within the course please refer to the Regulations for Academic Integrity at the University of Latvia. Within this course, the use of generative artificial intelligence (AI) tools is allowed in exceptional cases, if it has been specified and authorised in writing by the instructor of this course. In all other cases, submission of materials generated by the AI (text, images, audio, video, etc.) in independent and group assignments, test, examination or any other assessment is not permitted, submission of this type of material will be considered an unauthorised use of aids.