GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Information Security Management, PG_00063898		
Field of study	Informatics		
Date of commencement of studies	February 2026	Academic year of realisation of subject	2026/2027
Education level	second-cycle studies	Subject group	Optional subject group Specialty subject group Subject group related to scientific research in the field of study
Mode of study	Full-time studies	Mode of delivery	at the university
Year of study	1	Language of instruction	Polish
Semester of study	2	ECTS credits	3.0
Learning profile	general academic profile	Assessment form	assessment
Conducting unit	Department Of Software Engineering -> Faculty Of Electronics Telecommunications And Informatics -> Wydziały Politechniki Gdańskiej		
Name and surname of lecturer (lecturers)	Subject supervisor	dr hab. inż. Rafał Leszczyna	
	Teachers	dr hab. inż. Rafał Leszczyna	

Lesson types and methods of instruction

Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
Number of study hours	15.0	0.0	0.0	15.0	0.0	30

E-learning hours included: 0.0

Learning activity and number of study hours

Learning activity	Participation in didactic classes included in study plan	Participation in consultation hours	Self-study	SUM
Number of study hours	30	6.0	39.0	75

Subject objectives

The objective of this module is to develop understanding and to acquire knowledge related to information security and privacy issues from the perspective of system analyst

Learning outcomes

Course outcome	Subject outcome	Method of verification
[K7_U02] can perform tasks related to the field of study as well as formulate and solve problems applying recent knowledge of physics and other areas of science	Student understands basic concepts related to security risk analysis and protectionagainst security threats and can use these concepts while analysing a concrete IT system	[SU2] Assessment of ability to analyse information [SU4] Assessment of ability to use methods and tools [SU5] Assessment of ability to present the results of task
[K7_W10] knows and understands, to an increased extent, the basic processes occurring in the life cycle of equipment, objects and technical systems, as well as methods of supporting processes and functions, specific to the field of study	Students recognises enterprise information assets and corresponding threats. They organise the company's information assets according to the level of criticality. Students determine threats using attack trees. They define possible attack scenarios.	[SW3] Assessment of knowledge contained in written work and projects [SW1] Assessment of factual knowledge
[K7_W11] knows and understands, to an increased extent, the general principles of creation and development of forms of individual entrepreneurship and the economic, legal and other conditions of various types of activities related to the awarded qualification, including the principles of protection of industrial property and copyright law	Students recognises enterprise information assets and corresponding threats. They organise the company's information assets according to the level of criticality. Students determine threats using attack trees. They define possible attack scenarios.	[SW3] Assessment of knowledge contained in written work and projects [SW1] Assessment of factual knowledge

Subject contents	1.Information assets and their importance 2. Information and information security 3. Trust and security 4. Usable security 5. Information assets classification and labelling 6. Security threats and vulnerabilities 7. Selected security risk management techniques 8.Information Security Managment System (ISMS) 9. Selected security risk analysis techniques - attack trees 10. ISO/IEC 27001:2013 scope, requirements and compliance assessment 11. Privacy management 12. Security vs Safety vs Privacy 13. Development of secure software 14. Security of Industrial Automation and Control Systems (IACS)
Prerequisites and co-requisites	Previous participation in the module *Requirements Engineering*

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
Activity/presence	10.0%	10.0%
Written exam	45.0%	45.0%
Project	45.0%	45.0%

Recommended reading

Basic literature	1. ISO/IEC 27001 standard 2. IEC/ISA 62443 standards 3. Ross Anderson, Security Engineering, 2-nd edition (available online)
Supplementary literature	Standard NIST SP 800-53 Rev. 5 (available online)
eResources addresses	Adresy na platformie eNauczanie:

Example issues/ example questions/ tasks being completed

1. Analyse possible scenarios to achieve the attackers goal(s) in a target system.
2. Propose additional security controls that protect against identified attacks.
3. Provide an example of a form of an information asset.
4. Provide examples of 2 types of attributes that can be assigned to attack tree nodes.
5. Provide an example of loss of confidentiality of an information asset.
6. Should risk management be a cyclical process? Justify your answer.
7. Provide an example of transferring a cybersecurity risk.
8. What is the leading international standard for ISMS? Provide the entire identifier, including the letters and the number.
9. What is the recommended practice to address privacy concerns in products and business models?
10. Should the protection of user privacy embrace any principles? If it should, which ones?

Work placement	Not applicable

Document generated electronically. Does not require a seal or signature.