#### card of course

|  |  |
| --- | --- |
| Subject name | Data Security Management |

1. The placement of the subject in the study system

|  |  |
| --- | --- |
| 1.1. Field of study | Computer science |
| 1.2. Form and path of study | Full-time/Part-time |
| 1.3. Level of education | First-cycle studies |
| 1.4. Study profile | Practical |

|  |  |
| --- | --- |
| 1. 5. Specialty | Cybersecurity and computer forensics |
| 1.6. Subject Coordinator | Dr Mateusz Górka |

2. General characteristics of the subject

|  |  |
| --- | --- |
| 2.1. Belonging to a subject group | Optional/practical |
| 2.2. Number of ECTS | 6 |
| 2.3. Language of lectures | Polish |
| 2.4. Semesters in which the subject is taught | V |
| 2.5.Criteria for selecting course participants | For specializations: Cybersecurity and computer forensics |

1. Learning outcomes and course delivery
   1. Subject Objectives

|  |  |
| --- | --- |
| No. | Subject Objectives |
|
| C1 | Transfer of knowledge on data security management |
| C2 | Familiarization with the practical distinction and application of ISO 9001 type standards and the ISO/IEC 27001 standard |
| C3 | Familiarization with practical understanding and application of key data security management methods |
| C4 | Ensuring understanding of key processes implemented within data security management, including: implementing DLP systems, data mapping, creating security policies for data protection |

* 1. Subject-specific learning outcomes, divided into knowledge , skills and competences , with reference to the directional learning outcomes

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No. | Description of subject  learning outcomes | Reference to  directional effects  learning (symbols) | Method of implementation (mark "X") | | | |
| ST | | NST | |
| Classes at the University | Activities on  the platform | Classes at the University | Activities on  the platform |
| After passing the course, the student knows and understands **the knowledge** | | | | | | |
| W1 | The student knows the theoretical foundations of data security management | INF\_W15 INF\_W22 |  | X |  | X |
| W2 | The student knows the theoretical basis of conducting data loss risk analysis. |  | X |  | X |
| W3 | The student has general theoretical knowledge of data mapping in the enterprise as well as creating security policies. |  | X |  | X |
| W4 | The student has general theoretical knowledge of GDPR, as well as Information Security Management Systems. |  | X |  | X |
| W5 | The student has general theoretical knowledge of data monitoring, understands the application of the OSI model. |  | X |  | X |
| After passing the course, the student is **able** to: | | | | | | |
| U1 | The student is able to define key processes and methods of data security management. | INF\_U08 INF\_U16 INF\_U25 | X |  | X |  |
| U2 | The student is able to map data, conduct risk analysis, and propose security policies. | X |  | X |  |
| U3 | The student is able to characterize security monitoring, intrusion detection, security analysis using logs, event logs and collected statistics. The student is able to present the characteristics of wireless networks and mobile devices oriented to security. | X |  | X |  |
| U4 | The student is able to use tools for creating backup copies and restoring them. | X |  | X |  |
| After completing the course, the student is ready to take part in **social competences.** | | | | | | |
| K1 | Understands the need to develop knowledge about computer networks and their operating mechanisms. | INF\_K04  INF\_K05 | X |  | X |  |
| K2 | Is able to convey acquired knowledge in an understandable way. | X |  | X |  |
| K3 | Is able to use specialized software proficiently. | X |  | X |  |

3.3. Forms of teaching and their number of hours - Full-time studies (ST), Part-time studies (NST)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Path | Lecture | Exercises | Design | Workshop | Laboratory | Seminar | Lecturer | Classes conducted using distance learning methods and techniques in the form of a lecture | Other | **ECTS points** |
| **ST** | 20 |  |  |  | 40 |  |  |  |  | 6 |
| **NST** |  |  |  |  | 20 |  |  | 10 |  | 6 |

3.4. Content of education (separately for each form of classes: (W, ĆW, PROJ, WAR, LAB, LEK, OTHER). It should be marked (X) how the given content will be implemented (classes at the university or classes on the e-learning platform conducted using distance learning methods and techniques)

TYPE OF CLASS: LECTURE

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No. | Content of the course | Reference to subject-specific learning outcomes | Method of implementation (mark "X") | | | |
| ST | | NST | |
| **Classes at the University** | **Activities on  the platform** | **Classes at the University** | **Activities on  the platform** |
| 1. | Data security management, cybersecurity project management methods, risk and risk analysis methods, basic concepts and principles of CIA (confidentiality, integrity, availability) | W1, W2 |  | X |  | X |
| 2. | Enterprise Data Mapping, Data Security Policies – Creation and Implementation | W3 |  | X |  | X |
| 3. | Personal data protection and GDPR compliance. Information security management systems ISMS. Data security incident management. | W4, W5 |  | X |  | X |
| 4. | The OSI model and its importance for data security. Data security monitoring and auditing. | W5 |  | X |  | X |
| 5. | Summary of classes and discussion of grades |  |  | X |  | X |

TYPE OF CLASS: LABORATORY

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No. | Content of the course | Reference to subject-specific learning outcomes | Method of implementation (mark "X") | | | |
| ST | | NST | |
| **Classes at the University** | **Activities on  the platform** | **Classes at the University** | **Activities on  the platform** |
| 1. | Data mapping in the enterprise/ local government units. Analysis of the organizational structure, preparation of data projections, creation of a list containing the source, data classifications, keywords, storage methods. | U1, K1 | X |  | X |  |
| 2. | Conducting data loss risk analysis in the enterprise, creating security policies to prevent data loss. Communicating changes in the scope of implemented security policies | U2 | X |  | X |  |
| 3. | Security of protocols and devices of individual layers of the OSI model, network firewalls - firewall, VPN tunneling and IPsec protocol. - practical examples of solutions. Wireless networks and mobile devices - infrastructure security - practical examples of solutions. | U3 | X |  | X |  |
| 4. | Tools for creating backup copies of systems and data packages – practical examples of solutions.  Examples of DLP systems, application. | U4, K2, K3 | X |  | X |  |
| 5. | Summary of classes and discussion of grades |  | X |  | X |  |

3.5. Methods of verifying learning outcomes (indication and description of methods of conducting classes and verification of achievement of learning outcomes and method of documentation)

|  |  |  |  |
| --- | --- | --- | --- |
| Subject Effects | Teaching methods | Methods of verifying learning outcomes | Documentation methods |
| KNOWLEDGE | | | |
| W1-W5 | informative, conversational lecture with the use of multimedia | Using materials and content included in the lecture to pass the exam – 100% of the lecture grade | Examination sheet |
| SKILLS | | | |
| U1-U4 | Laboratory classes, problem solving, discussions | Final assignment - students create a secure VPN network connection between the client and the server and make backup copies of data and operating systems. They configure resource permissions - 100% of the lab grade. Alternatively, students map data for an example enterprise (the structure is given), then conduct a risk analysis of data loss or intentional processing, and make a proposal for implementing selected3 security policies. They present a proposal for communicating the implementation of security policies. | Task file |
| SOCIAL COMPETENCES | | | |
| K1-K3 | Laboratory classes, problem solving, discussions | Final assignment - students create a secure VPN network connection between the client and the server and make backup copies of data and operating systems. They configure resource permissions - 100% of the lab grade. Alternatively, students map data for an example enterprise (the structure is given), then conduct a risk analysis of data loss or intentional processing, and make a proposal for implementing selected3 security policies. They present a proposal for communicating the implementation of security policies. | Task file |

3.6. Assessment criteria for the achieved learning outcomes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Learning effect | For a grade of 3 or "pass."  the student knows and understands/is able to/is ready to | For a grade of 3.5, the student knows and understands/is able to/is ready to | For a grade of 4, the student knows and understands/is able to/is ready to | For a grade of 4.5, the student knows and understands/is able to/is ready to | For a grade of 5, the student knows and understands/is able to/is ready to |
| W | 51-60% of knowledge indicated in learning outcomes | 61-70% of knowledge indicated in learning outcomes | 71-80% of knowledge indicated in learning outcomes | 81-90% of knowledge indicated in learning outcomes | 91-100% of knowledge indicated in learning outcomes |
| U | 51-60% of skills indicated in learning outcomes | 61-70% of skills indicated in learning outcomes | 71-80% of skills indicated in learning outcomes | 81-90% of skills indicated in learning outcomes | 91-100% of skills indicated in learning outcomes |
| K | 51-60% of skills indicated in learning outcomes | 61-70% of skills indicated in learning outcomes | 71-80% of skills indicated in learning outcomes | 81-90% of skills indicated in learning outcomes | 91-100% of skills indicated in learning outcomes |

3.7. Literature

Basic

* “An Introduction to Information Security” (NIST SP 800-12) - National Institute of Standards and Technology (NIST), 2017. An Introduction to Information Security
* “Security and Privacy Controls for Information Systems and Organizations” (NIST SP 800-53) - National Institute of Standards and Technology (NIST), 2020. Security and Privacy Controls for Information Systems and Organizations
* “Bezpieczeństwo informacji — wprowadzenie” (NSC 800-12) - Narodowy Standard Cyberbezpieczeństwa, 2020. Bezpieczeństwo informacji - https://www.gov.pl/attachment/4b31f0bc-b5ab-4382-883a-2624bc2e54d6
* Kowalewski M, Kowalewski J. Zarządzanie bezpieczeństwem informacji organizacji, Oficyna Wydawnicza Politechniki Warszawskiej, 2024

**Supplementary**

* National Institute of Standards and Technology Security and Privacy Controls for Information Systems and Organizations” (NIST SP 800-53) - National Institute of Standards and Technology (NIST); CreateSpace; Scotts Valley; 2017
* “Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych” (NSC 800-18) - Narodowy Standard Cyberbezpieczeństwa, 2021. https://www.gov.pl/attachment/f561b58d-c915-4d88-8af3-0d3f71f14095
* Krzysztof Liderman, Bezpieczestwo Informacyjne, Wydawnictwo PWN 2018
* Andress J. Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie, Helion, 2021 [allegro]

4. Student workload - ECTS points balance

|  |  |  |
| --- | --- | --- |
| **Types of student activity** | **Student Load** | |
| **ST** | **NST** |
| **Classes requiring direct contact between the student and the academic teacher at the university premises** | **60** | **30** |
| Classes included in the study plan | 60 | 30 |
| **Student's own work** | **90** | **120** |
| Ongoing preparation for classes, preparation of project work/presentations/etc. | 45 | 60 |
| Preparation for passing classes | 45 | 60 |
| **TOTAL STUDENT HOURLY LOAD** | **150** | **150** |
| **Number of ECTS points** | **6** | **6** |

|  |  |
| --- | --- |
| Last change date | 30/09/2024 |
| The changes were introduced | INF Education Quality Team |
| The changes were approved | Arkadiusz Gwarda, M.A. |