Course Title	Information Security				
Course Code	DIS504				
Course Type	Elective				
Level	Postgraduate				
Year / Semester	1st / 2nd				
ECTS	7.5	**Lectures / week**	1	**Laboratories / week**	-
Course Purpose and Objectives	In the modern era of information technology, the security of information is of utmost importance. Organizations around the world are placing greater importance safeguarding their information systems and this has drastically increased the need for professionals in the field of information security. Protecting sensitive data no longer means just protecting the data, it also involves protecting various systems, controlling risks, legal actions and dealing with active hacking attempts. The Information Security (DIS504) course cover everything from policy to law, integrating advanced technical skills with administrative concepts. The course will familiarize students with information security governance not only on its technical aspects like cryptography, access control, intrusion detection, denial of service attacks, mitigation and forensics, but also on managerial and legal aspects. This course aims at ensuring competence in the protection of information systems while providing the student with appropriate skill sets in risk assessment, legal compliance, ethical issues and computer science forensic investigation. The students will, therefore, understand how to design, develop, implement and manage multifaceted security systems in different practical contexts after taking this course. Students will tend to think critically about modern security issues with the help of interactive lectures, case studies, assignments, and discussions. The objective of the course is to develop graduates with good technical skills and the ability to lead and manage security functions in any organization. DIS504 brings together theory and practice so that students are fully equipped to advance information security practice. The objectives of the course are: • Provide the fundamentals of Information security.				

<table>
<tr><td></td><td>

Present the information threats and attacks and ways to protect the information from such attacks.
Look at specific technical areas of information security such as authentication, access control, denial of service, intrusion detection and prevention systems and, finally cryptographic algorithms.
Concern with management aspects of information security and more specifically on management practices related to risk management.
Discuss the legal and ethical issues that are commonly found in today’s organizations.
Introduce computer forensics and how we can find evidence.

</td></tr>
<tr><td>Learning Outcomes</td><td>
After completing the course the students are expected to:

O[1] Explain the challenges and scope of information security;
O[2] Identify the common threats faced today;
O[3] Describe the access control mechanism used for user authentication and authorization;
O[4] Understand the importance of cryptographic algorithms used in information security;
O[5] Explain the use of such security tools as firewalls and intrusion prevention systems;
O[6] Recognize the importance of physical security and discuss ways to improve physical security of an enterprise;
O[7] Ensure infrastructure and network security;
O[8] Examine and resolve legal and ethical issues;
O[9] Enhance critical thinking and analysis skills through the use of case studies, research papers and small group exercises.

O[10] Strengthen research, writing and presentation skills.
<table>
<tr><td>1. Knowledge</td><td>C.L.O.[1] Describe fundamental elements of information security.

C.L.O.[2] Analyze the legal and ethical issues commonly found in today's organizations.

C.L.O.[3] Discuss computer forensics.</td></tr>
<tr><td>2. Skills</td><td>C.L.O.[4] Use specific technical aspects of information security, such as authentication,</td></tr>
</table>
</td></tr>
</table>

	access control, denial of service, attack detection and prevention systems, and finally, cryptographic algorithms. C.L.O.[5] **Practice** information security management aspects and, more specifically, practices related to risk management.
3. Competencies	C.L.O.[6] **Create** ways of protection from information attacks and any other threats.
(Responsibility and autonomy)	C.L.O.[7] **Propose** ways of finding evidence related to computer forensics.

Prerequisites	None	**Required**	None
Course Content	1st week: Introduction to Information Security. C.L.O.[1] – Describe fundamental elements of information security. 2nd week: Attacks and Threats. C.L.O.[1] – Describe fundamental elements of information security. C.L.O.[6] – Create ways of protection from information attacks and any other threats. 3rd week: Denial of Service Attacks. C.L.O.[1] – Describe fundamental elements of information security. C.L.O.[4] – Use specific technical aspects of information security, such as denial of service. C.L.O.[6] – Create ways of protection from information attacks and any other threats. 4th week: Intrusion Detection and Prevention Systems. C.L.O.[4] – Use specific technical aspects of information security, including attack detection and prevention systems. C.L.O.[6] – Create ways of protection from information attacks and any other threats. 5th week: Basic Cryptography. C.L.O.[1] – Describe fundamental elements of information security. C.L.O.[4] – Use specific technical aspects of information security, including cryptographic algorithms. 6th week: Access Control Fundamentals. C.L.O.[1] – Describe fundamental elements of information security. C.L.O.[4] – Use specific technical aspects of information security, such as access control.		

	7th week: User Authentication. C.L.O.[1] – Describe fundamental elements of information security. C.L.O.[4] – Use specific technical aspects of information security, such as authentication. 8th week: Physical Security. C.L.O.[1] – Describe fundamental elements of information security. C.L.O.[6] – Create ways of protection from information attacks and any other threats. 9th week: Risk Management. C.L.O.[1] – Describe fundamental elements of information security. C.L.O.[5] – Practice information security management aspects, including risk management. 10th week: Network Security. C.L.O.[1] – Describe fundamental elements of information security. C.L.O.[4] – Use specific technical aspects of information security, such as network security protocols. C.L.O.[6] – Create ways of protection from information attacks and any other threats. 11th week: Legal and Ethical Issues in Information Security. C.L.O.[2] – Analyze the legal and ethical issues commonly found in today's organizations. C.L.O.[1] – Describe fundamental elements of information security. 12th week: Introduction to Forensics. C.L.O.[3] – Discuss computer forensics. C.L.O.[7] – Propose ways of finding evidence related to computer forensics. 13th week: Conclusions / Rehearsal. C.L.O.[1] – Describe fundamental elements of information security. C.L.O.[3] – Discuss computer forensics. C.L.O.[5] – Practice information security management aspects. C.L.O.[7] – Propose ways of finding evidence related to computer forensics.
Teaching Methodology	Mix of interactive lectures, active learning techniques and activities. More precisely: • Interactive Lectures • Notes and PowerPoint Presentations in digital format through the electronic platform • Basic textbook(s) and additional bibliography • Assignments • Interactive Activities • Discussions in Forums through the electronic platform of real word case studies • Web links • Critical reflection on research article

<table>
<tr><td></td><td>

Peer review on group working and discussion in forum
Educational videos on real world case studies and critical discussion in forum

</td></tr>
<tr><td>Bibliography</td><td>
Compulsory Bibliography

W. Stallings, L. Brown, Computer Security Principles and Practice, 4th edition, 2018, Pearson
Wenliang Du, Computer & Internet Security: A Hands-on Approach
Michael E. Whitman, Principles of Information Security, 6th edition, 2018

Additional Bibliography

Yang, J.; Chen, Y.-L.; Por, L.Y.; Ku, C.S. A Systematic Literature Review of Information Security in Chatbots. Appl. Sci. 2023, 13, 6355. https://doi.org/10.3390/app13116355
Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping study. Arabian Journal for Science and Engineering, 45(4), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

</td></tr>
<tr><td>Assessment</td><td>
5% Quizzes
20% Projects/Assignments
10% Peer Assessment
5% Oral Presentation
60% Final exams
Assessment methods and mapping with Learning Outcomes
<table>
<tr><td></td><td>Percentage</td><td>O1</td><td>O 2</td><td>O3</td><td>O4</td><td>O5</td><td>O6</td><td>O7</td><td>O8</td><td>O9</td><td>O10</td></tr>
<tr><td>Quizzes</td><td>5%</td><td>√</td><td>√</td><td></td><td></td><td>√</td><td></td><td></td><td>√</td><td></td><td></td></tr>
<tr><td>Projects / Assignments</td><td>20%</td><td></td><td></td><td>√</td><td>√</td><td></td><td>√</td><td>√</td><td></td><td></td><td>√</td></tr>
<tr><td>Peer Assessment</td><td>10%</td><td></td><td></td><td>√</td><td>√</td><td></td><td>√</td><td>√</td><td></td><td>√</td><td>√</td></tr>
<tr><td>*Oral Presentation</td><td>5%</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>√</td><td>√</td></tr>
</table>
</td></tr>
</table>

	<table><tr><td>Final exam</td><td>60%</td><td>√</td><td>√</td><td>√</td><td>√</td><td>√</td><td></td><td></td><td>√</td><td></td><td></td></tr></table> *Oral presentation of a state of the art research paper or a case study in the field of "Information Security". List of papers or case studies to be announced during Week 4.
Language	English