Prince Sultan University
College of Computer and Info Sciences / Department of Information Systems
Semester 252 – AY(2025-2026)
Course Syllabus

1. Course number and name: CYS401: Fundamentals of Cybersecurity
2. Credits and contact hours: 3 (3,0,1)
3. Instructor's or course coordinator's name: Dr. Rabia Latif
    a. Scheduled Office Hours: 8:00-9:00 (U, M, T, W)
    b. Office Location: W355 c. Email: rlatif@psu.edu.sa

4. Text book, title, author, and year
    a. Primary Text: Cybersecurity Essentials Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short, (2018)
    b. Other References:
        - Bhusan, M., Rathore, R. S., & Jamshed, A. (2018). Fundamental of Cyber Security: Principles, Theory and Practices. BPB Publications.
        - CISSP: Certified Information Systems Security Professional Official Study Guide, 8th Edition, by Mike Chapple, James Stewart and Darril Gibson, ISBN-13: 978-1119475934, SYBEX, Wiley Brand.
    c. Electronic Materials: None
    d. Learning Management System: Moodle available at https://lms.psu.edu.sa

5. Specific course information
    a. Brief description of the content of the course (catalog description):
    This course serves as an introductory course to the Cybersecurity track whereby the basic concepts including cybersecurity in the business context, threats and attacks in different systems, cybersecurity authentication and authorization techniques, cybersecurity models and approaches, and the latest trends in cybersecurity. Besides, the course is designed to provide an overview and understanding of established cybersecurity strategy and offers students the opportunity to engage in strategic decision making in the context of cybersecurity.
    b. Prerequisites or corequisites: None
    c. Indicate whether a required, elective, or selected elective (as per Table 5-1) course in the program: Required

6. Specific goals for the course
    a. Specific outcomes of instruction. The student will be able to:
    CLO 1: Discuss the fundamental issues and techniques of cyber security.
    CLO 2: Analyze the security models and approaches for specific security needs.
    CLO 3: Distinguish the security principles and their legal, ethical and professional aspects.

CLO 4: Apply appropriate cybersecurity countermeasures to prevent, detect, react, and recover from simple attacks.

b. Explicitly indicate which of the student outcomes listed in Criterion 3 or any other outcomes are addressed by the course.

Course LOs #	Student Outcomes		
	Computer Science	Software Engineering	Information Systems
1	1	1	1
2	2	2	2
3	4	4	4
4	6	6	6

7. Brief list of topics to be covered

- **Introduction to Cybersecurity** **CLO 1**
  - Cybersecurity concepts
  - Cybersecurity objectives and Goal.
  - Cybersecurity Triad and System components
  - Critical Information characteristics in Cybersecurity
  -
- **Security Foundations and Principles** **CLO 2, CLO4**
  - Cybersecurity foundations and elements
  - Threat, Attack, Vulnerability, and countermeasures in Cybersecurity
  - Attacks Types in Cybersecurity and their countermeasure
  - Threats Modelling and STRIDE
  - Protection Mechanisms and Countermeasures
  - Cybersecurity Governance and Planning in Business

- **Data Security and Information Asset Protection** **CLO 2, CLO 3**
  - Information Asset and Information Asset Domain
  - Due Care vs Due Diligence
  - Information Classification and Classification Procedure
  - Governmental Classification vs. Commercial Classification
  - Data Labeling and Protection Mechanisms
  - Data Sanitization Techniques
  - Data ownership roles and responsibilities.
  - Data Protection Legislation and Regulations (GDPR, PDPA, etc)

- **Cryptography Fundamentals.** **CLO 1, CLO 4**
  - Basic Concepts of Cryptography
  - Cryptography Components and process
  - Symmetric vs. Asymmetric Cryptography

- Digital Signature and Data Integrity
- Public Key Infrastructure and Digital Certificate

- **Principles of Security Design** **CLO 1, CLO 2**
  - Security Architecture principles
  - Common Architecture Flaws and Security Issues
  - Protection Mechanism for Ensuring Confidentiality, Integrity, and Availability: Bounds, Process Isolation, and Confinement

- **Computer Architecture Security** **CLO 1, CLO 2**
  - Hardware Components & Protection Rings
  - Memory Protection Mechanisms
  - Firmware and Operating System Hardening
  - Input/Output Security and TEMPEST
  - Server- client Systems Security: Server-side Attacks and Client-side Attacks

- **Systems Architecture Security** **CLO 1, CLO 4**
  - Database Systems Security
  - Cloud Computing and Virtualization with security Aspects
  - Internet of Things security
  - Web-Based Systems security and OWASP Program
  - Mobile Devices Security

- **ICS/SCADA System Security for CPS** **CLO 1, CLO 4**
  - ICS/SCADA Systems Security
  - Vulnerability
  - Threats, challenges & countermeasures
  - Security requirements
  - Policies
  - Governance and Compliance
  - ICS/SCADA systems security in smart grid

- **Managing Identity and Authentication.** **CLO 1, CLO 4**
  - Access Control Models
  - Access Control Attacks
  - Controlling Access to Assets
  - Identification and Authentication
  - Implementing Identity Management
  - Biometric standards
  - Biometric applications
  - Authentication vs. Identification

8. Weight of Assessments

- Quizzes (CLO 1,2,3) 10%
- Major Exam (All CLOs) 20%
- Assignments (CLO 2,4) 10%
- Attendance 5%
- Project (All CLOs) 15%
- Final Examination (All CLOs) 40%

The Assessment dates can be seen on Moodle.

9. Additional Information

Plagiarism and Academic Dishonesty:
"Plagiarism can be defined as unintentionally or deliberately using another person's writing or ideas as though they are one's own. Plagiarism includes, but is not limited to, copying another individual's work and taking credit for it, paraphrasing information from a source without proper documentation, and mixing one's own words with those of another author without attribution. In addition, buying a paper or project, or downloading a paper from the Internet, and submitting them as your own are also plagiarism. The penalty for academic dishonesty will bring course expulsion and failure, or even suspension" (Academic Integrity and Syllabus Acknowledgement Form).

Attendance Policies:
The University attendance policy will be strictly followed.
Students that are regularly absent will be given DN warnings.
Students are expected to attend all class sessions and be in class on-time. Attendance is taken during the first 5 minutes of the class. Missing a class session is a student's responsibility. Missed classes will not be repeated. It is the student's responsibility to periodically check course website for course content, projects assignments, updates and notifications.

Exam Policies:
It is not possible to reschedule a major exam. If any student missed an assessment, the makeup will be at the end of the semester and all the materials are included (comprehensive assessment). Makeup exams will only be approved in limited cases as stipulated in the university bylaws. Generally, the final exam includes all material covered during the semester (comprehensive).

Assignment/Project Policies:
Students are expected to actively participate in class discussion, activities and online Forums. Students are expected to complete the class assignment and submit the answers during the concerned tutorial session. Late assignments are not accepted.