1. **Course Number and Course Title:**

   COE 594-12 – Usable Security and Privacy

2. **Credit Hours:**

   3 – 0 – 3

3. **Prerequisites and/or Co-Requisites:**

   Prerequisite: Approval of the CSE Head of Department
   Co-requisites: None
   Competencies: Undergraduate knowledge of security.

4. **Name and Contact Information of Instructor:**

   Name: Dr. Reham Aburas
   Email: raburas@aus.edu
   Office: ESB 2070
   Phone: 05 5362 7822
   Office Hours: Posted on office door and iLearn; also by appointment

5. **Course Description (Catalog Description):**

   Presents advancements in usable security and privacy, with a focus on designing secure, usable systems. Covers human-centered design principles and their application to security and privacy. Examines current research on topics such as authentication, mobile security, and social engineering threats. Includes topics on privacy, privacy ethics, and the security of new technologies.

6. **Textbook and other Supplemental Material:**

   Textbook:

   - Anderson R., *Security Engineering: A guide to Building Dependable Distributed Systems*, John Wiley & Sons, 3rd ed., 2020.

   Other supplemental material:

   - S. Garfinkel, and Lipford H. R., *Usable Security: History, Themes, and Challenges,* Morgan & Clay Pool Publishers, 1st ed., 2014.
   - Lazar J., Feng H. J., and Hochheiser H., *Research methods in human-computer interaction*, Morgan Kaufmann, 2nd ed., 2017.
   - Cranor L. F., and Garfinkel S., *Security and Usability: Designing Secure Systems that People Can Use,* O'Reilly Media Inc., 1st ed., 2005.
   - Course material will also be based on research papers listed below:
     - Distler V. et al*., A systematic literature review of empirical methods and risk representation in usable privacy and security research,* ACM Transactions on Computer-Human Interaction (TOCHI), 2021.
     - Klemmer J. H., et al*., "Make Them Change it Every Week!": A Qualitative Exploration of Online Developer Advice on Usable and Secure Authentication.,* ACM Conference on Computer and Communication Security, 2023.
     - Mathur, A., Kshirsagar M., and Mayer J*., What makes a dark pattern... dark? Design attributes, normative considerations, and measurement methods. Proceedings of the CHI conference on human factors in computing systems*, 2021.

- Garrido G. M., Vivek N., and Dawn S., *Sok: Data privacy in virtual reality,* Proceedings of the Privacy Enhancing Technologies Symposium (PoPETs), 2024.
- Yao Y., et al., *A survey on large language model (LLM) security and privacy: The good, the bad, and the ugly*, High-Confidence Computing, 2024.

7. Course Learning Outcomes:

Upon completion of the course, students will be able to:

1. Appraise the foundational principles of human-centered design for security and privacy.
2. Examine various authentication techniques and encryption methods that balance security with usability.
3. Evaluate the implications of permission models and transparency on user security.
4. Analyze current issues such as social engineering, privacy-enhancing technologies and privacy ethics.
5. Assess the future challenges in security and privacy associated with IoT devices and emerging technologies, including AR/VR and AI.
6. Conduct independent research in the field of usable security and privacy.

8. Teaching and Learning Methodologies:

Methods include lectures, academic paper reviews, case studies, class discussions, and group work. Students learning is assessed via homework assignments, paper reviews, team research project and exams.

9. Course Topics and Schedule:

Topic/Activity	**Weeks**
Introduction to Usable Security and Privacy	Week #1
Fundamentals of Human-Centered Designs – Research Methods	Week #2
Fundamentals of Human-Centered Designs – Evaluation Techniques	Week #3
Authentication in Smart Devices	Week #4
Usable Encryption	Week #5
Mobile Systems and Permission Models	Week #6
Transparency	Week #7
Social Engineering and Deceptive Designs – Phishing + Midterm exam	Week #8
Social Engineering and Deceptive Designs – Dark Patterns	Week #9
Privacy Enhancing Technologies	Week #10
Privacy Ethics	Week #11
Usable Security for IoT Devices	Week #12
Emerging Topics – AR/VR Security and Privacy	Week #13
Emerging Topics – AI for Security and Privacy	Week #14
Research Project Presentations	Week #15
Final Exam	Week #16

10. Schedule of Laboratory and other Non-Lecture Sessions:

The paper review is done individually and is due in Week #13. Students must conduct a review on a research paper that they choose from an assigned pool.
The research project is conducted by teams of two students and is due at the end of the semester. Student teams are required to propose a project related to usable security and privacy, and apply the knowledge and techniques acquired throughout the course to create a working demo. They

will submit a final short paper that outlines the techniques applied, explains the steps taken, and provides a thorough analysis of the results. Students will present the projects in the final week.

11. Out-of-Class Assignments with Due Dates:

Assignment	Due Date (tentative)
Homework 1: Fundamentals of human-centered designs	Week #3
Homework 2: Authentication and usable encryption	Week #6
Project proposal	Week #8
Homework 3: Social engineering and deceptive designs	Week #9
Homework 4: Privacy enhancing technologies	Week #11
Paper review	Week #13
Research project	Week #15

12. Student Evaluation:

Assessment	Weight	Due Date (tentative)
Homework	10%	Cf. Section 11
Project proposal	5%	Cf. Section 11
Paper review	10%	Cf. Section 11
Midterm Exam	20%	Week #8
Research project	25%	Cf. Section 11
Final Exam	30%	Week #16

13. Assessment Instruments:

Assessment	Course Learning Outcomes
Homework	O1-O2, O4
Project proposal	O6
Paper review	O5, O6
Midterm Exam	O1-O3
Research project	O6
Final Exam	O1-O5

14. Contribution of Course to Program Outcomes:

MSCoE Program Outcomes	Emphasis in this course	Course Learning Outcomes
1. Perform research emphasizing creativity, independent learning and scientific methods in a chosen area of computer engineering.	●	O1-O6
2. Apply advanced mathematics and engineering knowledge in identifying, formulating and solving engineering problems.	○	O1, O2
3. Select and use techniques, skills and modern tools necessary for research or professional practice.	◑	O1, O6
4. Communicate effectively.	○	O6
5. Recognize the need for, and engage in, lifelong learning.	○	O5, O6

6. Attend to professional and ethical responsibilities.	◑	O4, O6

Emphasis: ● High; ◑ Medium; ○ Low; Blank – Nothing Specific Expected

15. Letter Grade Policy:

Total (T)	Letter Grade
90 ≤ T	A
85 ≤ T < 90	A-
80 ≤ T < 85	B+
75 ≤ T < 80	B
70 ≤ T < 75	B-
65 ≤ T < 70	C+
60 ≤ T < 65	C
T < 60	F