Institute of Business Administration (IBA), Karachi
School of Mathematics & Computer Science

Course Outline
CSE-468: Information Security & Ethics

Course Title	Information Security & Ethics
Course Code	CSE428
Program	BS Computer Science
Credit Hours	3
Prerequisites	Operating Systems, Computer Communications & Networks
Instructor/Email	Waseem Arain/ warain@iba.edu.pk

Course Description

This course introduces foundational and advanced concepts of information security together with the ethical responsibilities of computing professionals. Security is treated as a socio-technical discipline encompassing cryptography, software, systems, networks, human factors, organizational practices, law, and ethics. Students develop adversarial thinking, risk analysis skills, and professional judgment required for secure system design and governance.

Course Learning Outcomes (CLOs)

By the end of the course, students will be able to:

- **CLO-1:** Explain foundational concepts of information security, threats, and security design principles.
- **CLO-2:** Analyze security failures by considering technical, human, organizational, and ethical factors.
- **CLO-3:** Apply core security mechanisms conceptually, including cryptography, access control, and network defenses.
- **CLO-4:** Evaluate ethical, legal, and societal implications of information security decisions.
- **CLO-5:** Communicate security risks and mitigation strategies effectively to technical and non-technical audiences.

Assessment Scheme (*Tentative*)

Component	**Weight**
Quizzes	10%
Activities & Exercises	20%
Mid-Term Examination	20%
Feature Article/Project/Research*	20%
Final Examination	30%

**** A separate document will delineate the details.***

CLO–PLO Mapping

CLO \ PLO	PLO-2	PLO-3	PLO-7	PLO-8	PLO-9
CLO-1	✓				
CLO-2	✓	✓		✓	✓
CLO-3		✓			
CLO-4				✓	✓
CLO-5			✓		

Weekly Teaching Plan (*Tentative*)

Wk	Topics / Activities
1	**Introduction to Information Security** *Topics:* • Scope of Information Security • State of Cybersecurity (2024–2025) • Evolution of Cyber Threats • Cybersecurity Career Pathways *Subtopics:* • Technical, human, and organizational security • Modern threat landscape • Historical evolution of attacks • Industry roles and certifications *Activity:* • Security breach news analysis
2	**Security Principles and Ethical Foundations** *Topics:* • Core Security Principles • Ethics in Information Security *Subtopics:* • CIA Triad • Authenticity and non-repudiation • Authentication, Authorization, Accounting (AAA) • Defense in depth, least privilege • Ethical theories (Utilitarianism, Deontology, Virtue Ethics) • ACM & IEEE Codes of Ethics • Privacy as a human right *Activity:* • Ethical dilemma case studies

3	**Identity and Access Management** *Topics:* • Identity Proofing & Authentication • Modern Access Models *Subtopics:* • MFA and passwordless authentication • Biometrics: security vs privacy • Single Sign-On (SSO) • Federated identity • Zero Trust fundamentals *Activity:* • MFA implementation and password testing
4	**Access Control Models and Privacy Ethics** *Topics:* • Access Control Systems • Privacy and Surveillance Ethics *Subtopics:* • Physical vs logical access controls • DAC, MAC, RBAC, ABAC • Policy design principles • GDPR, CCPA, global privacy laws • Surveillance ethics • Right to be forgotten *Activity:* • Access control policy design
5	**Network Security Fundamentals** *Topics:* • Network Architecture Security *Subtopics:* • Firewalls (packet filtering, stateful, NGFW) • VPNs • Network segmentation and VLANs • SDN security *Activity:* • Virtual firewall configuration (pfSense)

6	**Advanced Network Defense** *Topics:* • Detection and Monitoring *Subtopics:* • IDS / IPS • SIEM • Web Application Firewalls • Honeypots and deception • Network traffic analysis *Activity:* • Wireshark traffic analysis
7	**Wireless and Web Security** *Topics:* • Wireless Security • Secure Communications *Subtopics:* • WPA3 and Wi-Fi security • Web proxies and content filtering • DNS security (DNSSEC, DoH) • TLS/SSL and IPSec *Activity:* • Wireless security audit
8	**Cryptography and Blockchain** *Topics:* • Cryptography • Blockchain Security *Subtopics:* • Symmetric & asymmetric encryption • Hashing and digital signatures • PKI • Post-quantum cryptography (intro) • Blockchain fundamentals • Smart contracts • Cryptocurrency ethics *Activity:* • Encryption demo and blockchain exploration

9	**Cloud Security and Zero Trust** *Topics:* • Cloud Security • Zero Trust Architecture *Subtopics:* • IaaS, PaaS, SaaS • Shared responsibility model • Container security • CASB • Micro-segmentation • Continuous verification *Activity:* • Zero Trust architecture design
10	**AI as a Cybersecurity Threat and Defense** *Topics:* • AI-Driven Threats • AI for Defense • AI Ethics *Subtopics:* • Deepfakes (audio/video) • AI phishing and BEC • WormGPT / FraudGPT • Adversarial ML attacks • AI-powered SIEM and UEBA • Securing AI models • AI regulation and accountability *Activity:* • Deepfake creation & detection • Prompt injection testing
11	**Malware and Social Engineering** *Topics:* • Malware Threats • Human-Centered Attacks *Subtopics:* • Ransomware and APTs • Fileless and supply-chain attacks • AI-generated malware • Phishing, vishing, smishing • Psychological manipulation • BEC with deepfakes *Activity:* • Malware sandbox analysis • Phishing comparison exercise

12	**Risk Management and Security Assessment** *Topics:* • Risk Frameworks • Security Testing *Subtopics:* • Qualitative & quantitative risk • STRIDE, DREAD, PASTA • Vulnerability management • Pen testing vs audits • Red/Blue/Purple teams • Bug bounties *Activity:* • Risk register and vulnerability assessment
13	**Data Protection, Incident Response & BCP** *Topics:* • Data Governance • Incident Response • Business Continuity *Subtopics:* • Data classification and lifecycle • DLP and backups • Incident response lifecycle • Digital forensics basics • BIA, DRP, BCP • Ethical data handling (Pakistan context) *Activity:* • Incident response playbook • Breach scenario evaluation
14	**Legal, Regulatory, and Compliance** *Topics:* • International Cyber Law • Pakistan Cyber Laws • Governance *Subtopics:* • CFAA, DMCA, Budapest Convention • PECA 2016 & 2025 • NCSP-2021 • PISF-2025 • SBP, PTA, SECP regulations • NIST, ISO 27001, CIS Controls • Board-level security oversight *Activity:* • Legal comparison case study

Readings

- Pfleeger, Pfleeger, Margulies – *Security in Computing (5th Ed.)*(selected chapters)
- Ross Anderson – *Security Engineering (3rd Ed.)* (selected chapters)
- Floridi – *Ethics of Information*
- Nissenbaum – *Privacy in Context*
- *ACM Code of Ethics*
- NIST CSF, NIST SP 800-61/53
- MITRE ATT&CK
- GDPR, PECA 2016 (Pakistan)

Extended list of resources/readings will be made available as the course progresses.

Course Policies and Logistics

BYOD Course

We will engage in active learning. Please bring your laptop to each session to participate in simulations and hands-on activities and exercises.

Quizzes:

The course will place significant emphasis on various quizzes, including pop-up quizzes, take-home quizzes, and module quizzes. All quizzes will be conducted online, so having a smartphone or an appropriate computing device in class is essential to avoid losing quiz marks. While module quizzes follow a tentative schedule, other quizzes will be unannounced. The Kahoot! app will be used for quiz activities.

Activities and Exercises:

All activities must be submitted in the LMS (in the Assignments Folder created by us) based on the extent to which it has been completed, unless otherwise specified.

Any late or incomplete submissions should be uploaded to your Drop Box on LMS as soon as possible if you wish to provide an explanation for the delay later. However, please note that there is no guarantee that late submissions will be graded.

Mid-Term and Final Exams

Exams will be either partially or completely computer based. You are required to maintain a working laptop for the purpose which you will bring for the exams.

Make-up Exams

There will be no make-up exams for any reason whatsoever. Anyone who is allowed such an opportunity by the office, will be granted average of either the class or their own exam whichever is lower.

Attendance

Starting Spring 2025, the IBA Academic Council will enforce a mandatory attendance policy for all sessions in line with the established rules. It is your responsibility to monitor and adhere to these regulations.

Class conduct and regulations

Please consult the IBA code of conduct and related regulations for a comprehensive understanding of the topic.

However, any disruptive actions or attempts to undermine the productive learning environment established for the course—such as plagiarism, submitting fake or fraudulent work, or aiding such acts in quizzes or assignments—will result in a failing grade ('F') for the course. Additionally, further disciplinary actions may be initiated in accordance with the code of conduct.

Late submission and Makeup exams:

Late submissions will incur a 20% penalty for each day past the due date. Beyond this period, the assignment must still be submitted but will not receive any credit. However, in cases of medical emergencies supported by written documentation, the credit for that component will be transferred to the final weightage. Similarly, no makeup exams will be offered.

Office Hours:

I will be available during the following office hours for walk-in discussions regarding any course-related issues. Alternatively, you may schedule an appointment via email:

- Tuesday: 1:00 PM – 2:00 PM
- Wednesday: 10:00 AM – 12:00 PM
- Thursday: 1:00 PM – 2:00 PM

Communication:

A Discord server has been set up for communication: https://discord.gg/wRNUMYas (The link will be active for one week). All students are required to join for course/class-related updates and discussions. Any communication shared here will be considered official.

Tech and Tools

Apart from setting-up a VM (separate instructions will be provided) you will be required to install the following tools (APS) in your devices as they will be used during the course.

1. Kahoot! https://kahoot.com/
2. Miro https://www.miro.com/
3. Discord https://www.discord.com/
4. Packet Tracer https://www.netacad.com/cisco-packet-tracer
5. Wireshark https://www.wireshark.com/