1. Course Details

- **Course Code**: IT 246
- **Title**: IT Ethics and Cybersecurity
- **Credits**: 3
- **Program Name**: Bachelor of Information Management (BIM)
- **College**: Prime College, Nayabazaar, Kathmandu
- **Year**: 3
- **Semester**: 6
- **Course Leader**: Er. Sharat Maharjan
- **Email**: sharat.maharjan@prime.edu.np
- **Office Hours**: 11:30am - 2:00pm
- **Session**: AY2024
- **Planned Hours**: 60 hours (48 hours in class, 6 hours assessment support, 6 hours self-study)
- **Virtual Learning Environment (VLE)**: [Platform e.g., MS Teams]
- **Timetable**: Refer to Published Timetable

---

2. Learning Outcomes

Upon completing this course, students will be able to:

1. Understand core ethical principles and their application in IT and business settings.
2. Identify and manage cybersecurity threats, implementing digital forensics methods.
3. Recognize intellectual property issues and apply ethical considerations in decision-making.
4. Analyze and comply with cyber law provisions, particularly in the context of Nepal.
5. Special focus will be given to network scanning, sniffing, identifying common vulnerabilities in web applications (such as SQL Injection, XSS), phishing using social engineering toolkit labs, password cracking, firewall configuration and analysis labs, and incident response.

---

3. Skills and Knowledge Gained after Completing this Course

Skills	Knowledge
Ethical Decision-Making	IT and Business Ethics
Cybersecurity Fundamentals	Cyber Law and Intellectual Property
Threat Mitigation	Digital Forensics Techniques
Digital Evidence Handling	Cybersecurity Threats and Attacks

---

4. Detailed Course Content

Unit 1: An Overview of Ethics (5 Hours)

- **Topics**: Ethics, Business Ethics, Corporate Social Responsibility, Decision-Making in IT.
- **Objectives**: Recognize ethical issues in IT and apply ethical principles in professional settings.

Unit 2: Ethics for IT Workers and Users (5 Hours)

- **Topics**: Managing IT worker relationships, professionalism, ethical IT resource usage, privacy issues.
- **Objectives**: Foster ethical IT practices and address privacy and anonymity in IT.

Unit 3: Intellectual Property (6 Hours)

- **Topics**: Intellectual property rights, copyright, patents, trade secrets, plagiarism, reverse engineering.
- **Objectives**: Understand intellectual property laws and recognize ethical considerations in digital content.

Unit 4: Ethical Decisions in Software Development and Ethics of IT Organizations (5 Hours)

- **Topics**: Software quality, green computing, contingent work, outsourcing, whistleblowing.
- **Objectives**: Apply ethical principles in software development and organizational practices.

Unit 5: Fundamentals of Cybersecurity (6 Hours)

- **Topics**: Cybersecurity basics, risks, common cyberattacks, network poisoning, technical attacks.
- **Objectives**: Develop an understanding of cybersecurity, types of cyber threats, and mitigation techniques.

Unit 6: Personal Cybersecurity (5 Hours)

- **Topics**: Securing home computers, mobile devices, IoT devices, and account security.
- **Objectives**: Evaluate and enhance personal cybersecurity practices.

Unit 7: Social Engineering and Cyber Terrorism (5 Hours)

- **Topics**: Social engineering tactics, countermeasures, types of cyber terrorism, infrastructure impact.
- **Objectives**: Analyze social engineering techniques and learn to prevent cyber terrorism.

Unit 8: Digital Forensics (7 Hours)

- **Topics**: Digital forensic processes, evidence collection, data recovery, legal aspects of forensics.
- **Objectives**: Perform digital forensic investigations and understand evidence handling requirements.

Unit 9: Cyber Law in context of Nepal (4 Hours)

- **Topics**: Nepal’s Electronic Transaction Act, cybercrime regulations, IT policies.
- **Objectives**: Comprehend the legal framework for cybersecurity in Nepal.

---

5. Course Lesson Delivery

Unit	Week	Topics Covered	Session Type
Unit 1	1	Ethics overview, Corporate Responsibility	Lecture
Unit 2	2	IT Worker Relationships, Privacy	Lecture, Discussion
Unit 3	3	Intellectual Property, Copyright	Lecture

Unit 4	4	Software Quality, Whistleblowing	Lecture
Unit 5	5	Cybersecurity Fundamentals	Lecture, Lab Practice
Unit 6	6	Personal Cybersecurity	Lecture, Hands-on Lab
Unit 7	7	Social Engineering, Cyber Terrorism	Lecture, Group Activity
Unit 8	8-9	Digital Forensics Processes	Lecture, Practical Lab
Unit 9	10	Cyber Law in Nepal	Lecture, Group-Activity

---

6. Important Dates (Exams/Submission Deadlines)

- **Midterm Exam**: Week 5 – Theory Exam (2 Hours)
- **Lab Project Submission**: Week 8 – Cybersecurity Project Due
- **Final Exam**: Week 12 – Comprehensive Practical and Theory Exam (3 Hours)

---

7. Teaching and Learning Methods

This course is delivered through a combination of lectures, practical lab sessions, and case studies to strengthen ethical understanding and cybersecurity skills:

- **Lectures**: Core IT ethics and cybersecurity principles.
- **Practical Labs**: Hands-on labs in digital forensics and cybersecurity. Special focus on labs for network scanning, vulnerability testing, social engineering simulations, and password protection techniques.

---

8. Internal Assessment and Evaluation

Type	Title	Weight
Assignment	Ethics and Cybersecurity Reports	40%
Class Participation	Group Activities and Case Studies	10%
Midterm Exam	Written Theory Exam	25%
Final Exam	Comprehensive Practical Exam	25%

---

9. Academic Policies

- **Attendance**: 85% minimum required for eligibility in final assessments.
- **Late Submission**: Penalties apply unless prior arrangements are made.
- **Academic Integrity**: Strict adherence to plagiarism and honesty policies.

---

10. Resources and Support

- **Required Textbooks**:
    - *Ethics in Information Technology* by George W. Reynolds.
    - *Cybersecurity All-in-One for Dummies* by Joseph Steinberg.

- **Suggested Readings**:
    - *Ethics and Technology* by Herman T. Tavani.
    - Nepal’s *Electronic Transaction Act* and *Electronic Transaction Rules*.
- **Student Support Services**: Contact faculty advisors for additional support.