Unit 1: Ethics & IT Ethics (10 Hrs.)

1. What is Ethics?

- Ethics refers to **moral principles** that govern behavior.
- It helps distinguish between **right and wrong** in decision-making.
- **Example:** A software company following **fair hiring practices**.

2. Corporate Social Responsibility (CSR)

- Companies **self-regulate** their impact on society.
- **Three key areas: Economic, Social, Environmental** responsibility.
- **Example:** Google investing in **renewable energy**.

3. Ethical Considerations in Decision Making

- **Transparency**: Open communication about policies.
- **Fairness**: Equal treatment of employees and customers.
- **Privacy**: Protecting user data from misuse.
- **Example:** Facebook handling **user data privacy issues**.

4. IT Worker Relationships & Professionalism

This means how IT workers behave professionally at work.

1. Professional Codes of Ethics

- These are **rules** that IT workers follow to do the **right thing**.
- Example: A software engineer should **not steal or sell user data**.

2. Professional Organizations

- Groups that support **good behavior** in IT.
- **IEEE & ACM** are two major IT organizations that set **ethical rules**.
- Example: **IEEE** says engineers should build **safe and useful** technology.

3. Certifications & Licensing

- A **certificate** proves that a person is **skilled and ethical** in IT.
- Example: **CISSP** is a certification that proves a person is a **trusted cybersecurity expert**.

Unit 2: Cyberattacks, Cybersecurity & Cyber Law (12 Hrs.)

5. CIA Triad (Confidentiality, Integrity, Availability)

- **Confidentiality** – Protecting sensitive data.
  - **Example:** Using **passwords & encryption**.

- **Integrity** – Ensuring data remains unchanged.
  - **Example: Checksums, Digital Signatures**.

- **Availability** – Ensuring data is accessible when needed.
  - **Example: Backup servers, Redundant systems**.

6. Common Cyber Attacks

- **Phishing** – Fake emails to steal login info.
  - **Example:** A user gets a **fake PayPal login email**.

- **Malware** – Software designed to harm systems.
  - **Example: Ransomware locks files** until a ransom is paid.

- **DDoS Attack** – Overloading a website to crash it.
  - **Example:** A hacker floods a gaming server, making it **unplayable**.

7. Incident Response Process (Handling a Cyber Attack)

When a cyber attack happens, IT teams follow **four steps** to fix it.

1. **Incident Notification**
   - Inform the security team about the attack.
   - Example: A company gets hacked → IT team is alerted.

2. **Protection of Evidence**
   - Keep records (logs) to **investigate** what happened.
   - Example: Checking which files were **changed or stolen**.

3. **Containment & Eradication**
   - Stop the attack and remove the threat.
   - Example: **Blocking the hacker's IP address** and deleting the malware.

4. **Follow-up**
   - Learn from the attack and improve security.
   - Example: If an employee **clicked a phishing email**, train them to **avoid future scams**.

8. Cyber Law of Nepal & Electronic Transaction Act

- Defines **legal actions against cybercrimes**.
- Covers **hacking, identity theft, and data breaches**.
- **Example:** A person spreading **false information online** can be punished under this law.

Unit 3: Privacy & Freedom of Expression (10 Hrs.)

9. Privacy Laws & Protection

- Protects user **personal data** from misuse.
- **Example:** GDPR (Europe) and **Cyber Law of Nepal** enforce data privacy.

10. Workplace Monitoring & Surveillance

Companies **watch employees' computer activities** to make sure they work properly.

- **Why?**
  - To **prevent time-wasting**.
  - To **protect company secrets**.
  - To **detect security risks**.
- **Example:**
  - Companies use **keylogging software** to track what employees **type on their keyboard**.
  - If an employee **leaks company passwords**, the software **records it**.

11. Freedom of Expression & Key Issues

Freedom of expression means **people can share their opinions** freely, but there are **some limits**.

1. First Amendment (USA)

- Protects **free speech** but does **not allow harmful speech**.
- **Example:** You **can criticize** the government, but you **can't make death threats**.

2. Social Media Censorship

- Social media platforms **control what people can post**.
- They **remove harmful content** like **hate speech, fake news, and violence**.
- **Example:**
  - **Facebook bans hate speech** to prevent online bullying.
  - **Twitter removes fake news** to stop misinformation.

Unit 4: Intellectual Property (8 Hrs.)

12. What is Intellectual Property (IP)?

Intellectual Property means **creations of the mind** that people legally own.

Types of Intellectual Property:

1. **Copyright** – Protects **books, music, movies, and software**.
    - Example: You **can't copy-paste** a book and sell it.

2. **Patent** – Protects **new inventions**.
    - Example: Apple patents **Face ID technology**.

3. **Trade Secret** – Protects **company secrets**.
    - Example: The recipe of **Coca-Cola** is a trade secret.

4. **Trademark** – Protects **logos & brand names**.
    - Example: You **can't copy McDonald's logo** for your own restaurant.

13. Intellectual Property Issues

- **Plagiarism** – Copying work without credit.
- **Reverse Engineering** – Analyzing a product to copy it.
- **Open Source Code** – Free-to-use code but may have **licensing rules**.
- **Example:** A company copying **Windows OS** and selling it illegally (**Piracy**).

Unit 5: Ethics in Software & IT Organizations (8 Hrs.)

- **Software ethics** means writing software that is **fair, safe, and doesn't harm people**.
- Example: A banking app **shouldn't steal customer money**.

14. Common Ethical Issues in Software:

1. **Privacy** – Apps should **not collect user data** without permission.
2. **Security** – Software should be **protected from hackers**.
3. **Plagiarism** – Developers should **not copy code** without permission.

15. What is Software Quality?

Software **quality** means the software **works well, is secure, and is easy to use**.

Key Features of High-Quality Software:

1. **Reliability** – The software **doesn't crash** often.
    - Example: **Microsoft Word** rarely crashes.

2. **Security** – The software **is hard to hack**.
    - Example: **Banking apps** use **encryption** to protect money.

3. **User-Friendly** – The software **is easy to use**.
    - Example: **Google Chrome** is simple and smooth.

16. Outsourcing & H-1B Visa Workers

- **Outsourcing** – Hiring developers from another country.
- **H-1B Visa** – Allows hiring skilled foreign workers.
- **Example:** Google hires **Indian engineers** on H-1B visas.

17. Whistle-Blowing & Green Computing

- **Whistle-Blowing** – Reporting unethical practices.
    - **Example:** A Facebook employee exposes **privacy violations**.
- **Green Computing** – Using IT to reduce environmental harm.
    - **Example:** Google using **energy-efficient data centers**.