Week no 7

Intellectual Property Rights (IPR) – Summary

What is Intellectual Property?

Intellectual Property Rights protect valuable creations and information, especially in software and technology.

They cover both digital data and related materials like manuals, documentation, and web content.

Proper protection is important to prevent misuse and financial loss.

Main Types of Intellectual Property

- Confidential Information
- Patents
- Copyright
- Trade Marks
- Designs

Confidential Information

- Information that is not public knowledge.
- Can include personal data, trade secrets, or sensitive business information.
- Protection applies only if the information is truly confidential.

Conditions for breach of confidence:

torny wala

- Information must be confidential.
- It must be shared under an obligation of confidence.
- There must be actual or expected unauthorized use or disclosure.

Patents

A patent gives an inventor exclusive rights to use or sell an invention for a fixed time.

Even independent inventors can be excluded if a patent exists.

Requirements for a patent:

- The invention must be new.
- It must involve an inventive step
- It must be usable in industry.
- It must not fall under excluded subject matter.

Software and patents:

Pure software is not patentable.

Software that produces a technical effect beyond normal hardware interaction can be patented.

Copyright

- Gives creators exclusive legal rights over their work.
- Protects computer programs, manuals, diagrams, and business documents.
- Internet use has increased risks of copying and piracy.

Exclusive rights include:

- Copying the work.
- Issuing copies to the public.
- Renting or lending.
- Public performance or display.
- Broadcasting.
- Making adaptations.

Acts Permitted Under Copyright

Some actions are allowed even without permission, such as:

- Fair dealing.
- Making backup copies of software.
- De-compilation for interoperability.
- Error correction.
- Certain database uses.

Remedies for Copyright Breach violation

- Civil remedies include injunctions, damages, and seizure of infringing copies.
- If the infringer did not know copyright existed, damages may not be awarded.
- Owners can enter premises without force to seize illegal copies.

Plagiarism

Using someone else's work or ideas as your own.

Examples of plagiarism:

- Submitting another person's work.
- Copying without credit.
- Incorrect citation.
- Rewriting with same structure.
- In programming, only changing variable names without changing logic.

Week no 8

Computer Contracts – Key Points & Highlights

1. What is a Contract?

A **legal agreement** between two or more parties

It specifies:

- ✓ Rights and duties of each party
- ✓ Purpose and goals of the agreement
- ✓ How issues during the contract will be handled
- ✓ Methods of termination and consequences

Highlight: Well-drafted contracts prevent disputes; unclear contracts create problems.

---

2. Importance of Clear Contracts

- Contracts should be **clear, concise, and unambiguous**.
- Ambiguity leads to:

- ✓ Unsatisfactory performance
- ✓ Disputes
- ✓ Waste of time and money

- Contract law exists to resolve unfair or harsh contract issues.

---

3. Contracts for Custom-Built Software (Fixed Price)

- Usually based on **standard form contracts** reused by suppliers.
- Structure includes:

- ✓ Introductory section
- ✓ Standard terms & conditions
- ✓ Annexes / appendice

---

4. Introductory Section

- Names and registered addresses of parties

- Date and authorized signatures
- Definitions of key terms (e.g., *Company*, *Client*)

---

5. Terms, Conditions & Annexes

- Annexes may include documents like **SRS (Software Requirements Specification)**.
- Prevents informal promises (e.g., by sales staff) from becoming legal obligations.

---

6. Issues Covered in Standard Terms & Conditions

- What will be produced and delivered
- Ownership of intellectual property
- Payment terms
- Delay and change calculations
- Penalty clauses
- Client obligations
- Standards and methods of work
- Progress meetings & project managers
- Acceptance procedures
- Warranty and maintenance
- Contract termination

---

7. Other Types of Software Service Contracts

There are **four main types**:

a. Fixed Price

- Cost decided in advance.
- Supplier bears risk of overruns.

b. Contract Hire

- Supplier provides staff.
- Staff work under client's direction
- Supplier only ensures competent staff.
- Paid per man-day.
- No acceptance tests or delay penalties.

c. Time and Materials

- Mix of fixed price and contract hire.
- Payment based on actual work done
- May include a maximum cost limit.

d. Consultancy Contracts

- Consultants analyze and suggest improvements.
- Output usually a **report**.
- Simple contracts, often fixed price

Exam Highlights ⋆

- Contracts prevent disputes.
- Fixed price vs time & materials is a **risk difference**.
- Annexes protect against verbal promises
- Contract hire focuses on **people**, not product.
- Consultancy contracts are **simpler** than development contracts.

Week no 9

Overview

The lecture focuses on **software safety**, **legal liability**, and **professional practices** in the development of **computer-controlled systems**, especially where failures can cause harm.

Why Software Safety Matters

Computer-controlled systems are widely used in **high-risk domains**, including:

- ✓ **Industry:** Manufacturing systems, robots
- ✓ **Medicine:** Intensive care monitoring, radiotherapy
- ✓ **Transport:** Railway signaling, aircraft, space shuttles

- **Military & Defense systems**

Failures in these systems can lead to **serious injury, loss of life, or property damage**.

Regulatory Issues in Software Safety

Key mechanisms used to regulate hazardous software systems:

1. Standards

- Established guidelines to ensure safety and quality
- Traditional and widely used method of regulation

2. Certification & Licensing

- **Certification:** Product or professional meets defined standards
- **Licensing:** Product or practitioner cannot operate without approval

3. Professional Codes of Practice

- Developed by professional and trade associations
- Guide ethical and safe behavior of practitioners

4. Regulation by Law

- Legal requirements enforce safety
- Fear of litigation encourages compliance with standards and licenses

---

Legal Liability

Product Liability

- Manufacturers, designers, and suppliers are responsible for harm caused by defective products
- Applies **even if contractual liability is limited**

Governed by:

✓ Consumer Protection Act (CPA) 1987
✓ Common law of negligence

Negligence

Occurs when:

- Designers or engineers fail to take **reasonable care**
- Poor design or construction leads to system failure and injury

---

Competence, Training & Experience

- **Competence:** Knowledge + ability to apply it correctly
- Assumption: Engineers working on safety-critical systems are competent

Important factors:

✓ Proper training
✓ Relevant professional experience

Factors Affecting System Safety

Key activities that contribute to safe systems:

- Hazard analysis
- Clear requirements and specifications
- System reliability and safety engineering
- Careful design
- Thorough testing and debugging
- Safety integrity analysis & risk assessment
- Proper documentation

Key Takeaways

- Software safety is **critical in safety-critical systems**
- Engineers have **legal and ethical responsibilities**
- Compliance with standards, laws, and professional practices reduces risk
- Competence and rigorous engineering processes are essential for safety

---

WEEK NO 10

Computer Misuse & Criminal Law – Summary

Introduction

- Computer-related crimes have increased rapidly due to widespread use of computers and the Internet.
- Media frequently reports large-scale computer frauds.

Major threats exist to:

- ✓ Commercial organizations
- ✓ Government databases
- ✓ Financial institutions
- ✓ National security

Computing and Criminal Activity

- Modern businesses heavily depend on computer systems (software and hardware).
- Growth in computer usage has led to a rise in cybercrime.
- The Internet has introduced new security risks and vulnerabilities.
-

Categories of Computer Misuse

- (Identified by the English Law Commission)
- Computer fraud
- Unauthorized access to computer systems
- Computer hacking
- Eavesdropping (spying on computer communications)
- Unauthorized use of computers for personal benefit
- Unauthorized alteration or destruction of data
- Denial of access to authorized users
- Unauthorized removal of stored information

Computer Fraud

Definition:
Dishonest manipulation of a computer or the Internet to gain money, property, or advantage, or to cause loss.

Types of Computer Fraud:

1.Input Fraud

Entering false or altered data intentionally.

2.Output Fraud

Stealing or misusing computer output (e.g., reports, results).

3.Program Fraud

Unauthorized modification of computer programs

Unauthorized Access to Computers

- Accessing a computer system without the owner's permission.
- Commonly known as **computer hacking**.

Purpose may include:

✓ Stealing data
✓ Altering information
✓ System manipulatio

Other Forms of Misuse

- **Eavesdropping**

Secretly listening to or spying on computer communications.

- **Unauthorized Use for Personal Benefit**

  Authorized users (often employees) misuse access for personal gain.

Key Highlights

- Computer misuse is a serious legal issue under criminal law.
- Fraud, hacking, and unauthorized access are the most common cybercrimes.
- Employees with legitimate access can also commit misuse.
- Laws aim to protect data, systems, and users from abuse.
-

Week no 11

Key Points & Highlights

1. Impact of Computerization

- Computerization has dramatically changed how information is stored, processed, retained, and shared.
- Data has become a **valuable commodity** with commercial importance.
- Businesses benefit from **easy, fast, and secure global data transfer**.

---

2. Data Protection vs Privacy

- **Data Protection**

  Concerns how organizations collect, use, and safeguard personal data.

  Focuses on protecting customer and employee information from misuse.

- **Privacy**

  A legal or policy-based right allowing individuals to control who can access their personal information

  Emphasizes secrecy and personal control over data.

---

3. Impact of the Internet

- Early data protection laws targeted threats from **centralized databases**.
- The Internet and World Wide Web introduced **decentralized and global data flows**.
- Raises concerns about whether traditional data protection laws can effectively regulate online activities.

---

4. Challenges in Regulating Data Processing

Regulation is complex due to:

1.Rapid technological advancement

2.Global nature of data processing

3.Differences in legal systems across countries

Enforcement is difficult because data systems are:

1.Highly advanced

2.Widely distributed

3.Constantly evolving

4.Used by powerful corporate and government entities

---

5. Convergence of Data Protection Practices ak Jasa huna

- International agreements and national laws are becoming more aligned.
- Emergence of **data protection principles** and **fair-use guidelines**.
- These principles help **harmonize data protection laws globally**.

---

6. Defamation and Protection of Reputation

- Digital networks enable fast and wide dissemination of information—true or false.
- Individuals may suffer reputational harm due to false statements shared online
- **Defamation laws** provide legal remedies for damage to reputation.
- Most countries recognize the right to protection of personal integrity and reputation.

⋆ Overall Highlight

The digital age has increased the value and vulnerability of personal data, making **data protection, privacy, and defamation laws essential** to balance technological progress with individual rights.

Week no 12

Introduction to Hacking

- **Hacking** is the attempt to gain **unauthorized access** to computer systems or resources.
- It can also mean **modifying a system** to achieve goals beyond its original purpose.

Who is a Hacker?

- A hacker is someone who **develops, modifies, or bypasses computer security**.
- Hackers usually have **advanced knowledge of hardware and software**.
- Hacking can be **ethical (legal)** or **criminal (illegal)**.
- Criminal hackers create **malware or spyware** to steal confidential data.

Types of Hacking

Website Hacking: Taking control of a website from its owner.

Network Hacking: Collecting network details like IP address and open ports.

Password Hacking: Recovering passwords using:

Brute force method (trying all combinations)

Dictionary attack (using predefined passwords)

Software Hacking: Modifying software features, such as converting demo versions into full versions.

Ethical Hacking: Finding system weaknesses legally and fixing them.

Email Hacking: Unauthorized access to email accounts.

Computer Hacking: Viewing, editing, or deleting files without permission.

Ethical Hacking (White Hat)

Done **with permission** to improve security.

Used to:

Test system security

Find vulnerabilities

Recover lost data

Ethical hackers help organizations **prevent real attacks**.

What to Do After a System is Hacked

- Turn off the system immediately.
- Disconnect it from the network.
- Restore from backup or reinstall software.
- Reconnect to the network after recovery.
- Inform authorities if required.

Tools of Hacking

Scanners: Detect security weaknesses in systems.

Telnet: Allows remote system access via terminal.

FTP: File Transfer Protocol, sometimes misused for hacking (uses port 21).

Computer Security Ethics

- Ethics is not based only on **feelings, religion, or law**.
- Ethical behavior depends on **values and responsibility**.
- Engineers and IT professionals should prioritize **public safety and trust**.

Penetration Testing

- Legal attempt to break into a system to find weaknesses.
- Tester reports vulnerabilities only.

Penetration Testing Models

White Box: Tester has full system information.

Black Box: Tester has no prior information.

Gray Box: Tester has partial information.

Hackers' Code of Conduct

Hacker Creed (Steven Levy)

- Free access to information.
- Hands-on learning.
- Mistrust authority.
- Judge hackers by skills, not status.

- Computers can improve life.

New Code of Ethics (Steven Mizrach)

- Do no harm.
- Protect privacy
- Leave no traces.
- Share knowledge.
- Use hacking to improve security.

Certified Ethical Hackers (CEH)

- Certification by **EC-Council**.
- Covers **21 security domains**.
- Ethical hackers often work in **Red Teams**.
- Focus on penetration testing and security assessment.

Week no 13

Information Security Practices (Lecture 13)

Introduction

- **Information Security (InfoSec)** is the practice of protecting information from:

  Unauthorized access

  Use or disclosure

  Modification or destruction

- It applies to **all forms of data**, including electronic and physical information.
- Main goal is to **protect data and ensure trust in systems**.

CIA Principles of Information Security

The foundation of information security is the **CIA Triad**:

1. Confidentiality

Ensures information is accessed **only by authorized users**.

Prevents data leakage and privacy breaches.

Examples: passwords, encryption, access control.

2. Integrity

Ensures information remains **accurate and unchanged**.

Protects data from unauthorized modification.

Examples: checksums, hashing, version control.

3. Availability

Ensures information is **accessible when needed**.

Protects against system failures and denial-of-service attacks.

Examples: backups, redundancy, maintenance.

Information Security Organizational Structure

Defines **roles and responsibilities** for information security.

Helps organizations manage and enforce security policies.

Ensures accountability and proper control of information assets.

Information Classification

Process of categorizing information based on **sensitivity and importance**.

Types of Classification

Government Classification: Public, Confidential, Secret, Top Secret.

Private Sector Classification: Public, Internal, Confidential, Restricted.

Classification Criteria

Value of information

Legal and regulatory requirements

Impact of data disclosure or loss

Key Highlights for Exams

InfoSec protects information in **all forms**.

CIA Triad is **core to information security**.

Confidentiality, Integrity, and Availability must be balanced.

Classification helps apply **appropriate security controls**.

Organizational structure supports **effective security management**.

Week no 14

Risk Management (Lecture 14)

Introduction

- **Risk Management** is the process of **identifying, evaluating, and reducing risks** to an organization.
- It helps protect **assets, information, and operations** from potential threats.
- Risk management is a **continuous and cyclical process**, not a one-time activity.

Overview of Risk Management

Systematic method to handle **potential risks** in any activity or project.

Organizations must:

Know what assets they have

Identify possible threats

Understand how well assets are protected

Detect security gap

Systematic method to handle potential risks means a planned way to identify, control, and reduce possible future problems in any activity or project.

Focus is on **minimizing damage and uncertainty**.

Risk Identification

This step identifies what can go wrong.

Key Elements

Assets: Valuable items like data, systems, people.

Threats: Events that can cause harm.

Threat Sources:

Man-made (hackers, errors)

Natural (floods, earthquakes)

Vulnerabilities: Weaknesses in systems or processes.

Controls / Safeguards: Measures used to protect assets.

Risk Assessment

Evaluates the **impact and probability** of risks.

Main Factors

- ✓ Potential loss if a risk occurs
- ✓ Effectiveness of existing controls
- ✓ Level of uncertainty
- ✓ Likelihood of threat occurrence
- ✓ Consequences or damage caused

Risk Control Strategies

Applied after assessing risks to reduce or manage them.

Types of Controls

Policies: Rules and guidelines.

Programs: Training and awareness initiatives.

Technical Controls: Firewalls, antivirus, access control

Key Highlights for Exams

Risk management is **ongoing and cyclical**.

Identification comes before assessment.

Risk assessment focuses on **likelihood and impact**.

Controls reduce **residual risk**.

Effective risk management protects organizational assets.

Week no 15

Social Networking & Ethics – Key Points

1. Introduction

- Social networking connects **people or organizations** through relationships like friendship, work, or information sharing.
- Similar to computer networks, but focuses on **social connections** rather than machines.
- Topic covers **benefits, risks, and safety measures** for users and children.

---

2. Social Networking Platforms (Web 2.0)

Facebook & MySpace – social networking sites.

Twitter – microblogging (short messages).

Blogs – online journals.

YouTube & Flickr – video and photo sharing.

Podcasts – downloadable audio content.

---

3. The Good, the Bad, and the Ugly

Good: Easy communication, information sharing, and networking.

Bad: Fraud, phishing, identity misuse.

Ugly:

Scammers impersonating users to steal money.

Personal information exposure (e.g., MI6 chief exposed through Facebook photos).

---

4. How to Protect Yourself Online

Keep private information private:

Avoid sharing address, phone number, SSN, financial details, full birth date, or daily schedule.

Security awareness:

Don’t click suspicious links.

Avoid installing unknown apps or add-ons.

Use strong, unique passwords.

Never reuse the same password for email and social media.

Account safety:

Review and lock privacy settings.

Accept only known friends

Be cautious of strangers.

Use antivirus software.

Google yourself to see what information is public.

Remember: **Social media is public—like a billboard in cyberspace**.

---

5. How to Protect Children

Be aware of **who children communicate with online**.

Know **age restrictions**:

Facebook & MySpace: **13+**

Twitter: **Open to all**

Encourage supervision, awareness, and safe online behavior.

---

6. Overall Message

Social networking offers benefits but carries **ethical and security risks**.

Awareness, privacy control, and responsible use are essential for **personal and child safety online**.

Week no 16

Lecture 16 – Key Points & Highlights

1. Introduction

Widespread internet use by individuals and organizations raises **moral, social, and ethical concerns**.

Common issues include:

Websites containing **incorrect or misleading information**

Online bullying via email, chat, and messages

Access to **inappropriate or illicit content**

Spreading **rumors** online

Using email for sensitive matters where face-to-face communication is better

---

2. Moral Issues

Plagiarism (copying others' work without credit)

Spam emails wasting users' time

Monitoring employees' internet and email usage

Using someone else's Wi-Fi without permission

Photo editing/manipulation that distorts reality

---

3. Ethical Issues

Easy access to **offensive, illegal, or unethical material**

Privacy violations

Online gambling addiction

Obesity and health issues linked to excessive internet use

Addiction to computer games

Digital divide – increasing gaps between rich and poor individuals/countries

---

4. Social Issues

- Companies moving **call centers abroad** to reduce costs
- Growth of **e-commerce** causing local shops to close
- Some countries **control or censor information**, limiting freedom of access
- Lack of proper policing means **online information may be inaccurate**

---

5. Advantages of the Internet

- Blogs and chats help **communities discuss local issues**
- Reduces isolation of **housebound individuals**
- Creates **employment opportunities**
- Easy access to advice and support services online

---

6. Disadvantages of the Internet

- **Reduced social interaction** due to online activities
- Closure of **local shops** because of online shopping
- Difficulty in fully controlling offensive content despite laws and filtering software
- Content may be offensive even if not illegal

---

7. Ownership and Control of the Internet

- The internet is **not owned by anyone**
- Governments increasingly **control or restrict access**
- Lack of strict regulation leads to **unchecked and unreliable information**

Overall Highlight

The internet offers major benefits but also introduces **serious moral, ethical, and social challenges**. Responsible use, awareness, and regulation are essential to reduce its negative impacts.
