Unit I: Introduction to Information Security (6 hours)

---

1. Definition of Information Security

- **Information Security (InfoSec)** means **protecting information** (data, files, communications) from **unauthorized access, modification, disclosure, or destruction**.
- It ensures that only the right people can access the right information at the right time.

☞ Example:

- When you log in to Facebook, your password protects your account. This is information security.
- If someone hacks it, that's a security breach.

History of Information Security

Information security didn't just start with computers – people have always needed to protect important information. The history can be divided into **three phases**:

---

1. Pre-Computer Era (Before 1960s)

- People protected information using **physical security** and **secret codes**.
- Kings and militaries used **cryptography (secret writing)** to hide messages.
    - Example: **Caesar Cipher** (shift letters by 3 places).
    - Example: **Enigma Machine** used by Germany in World War II.
- Information security was mostly about **paper documents, safes, and locks**.

☞ *Key point:* Security = physical + coded communication.

---

2. Early Computer Era (1960s – 1980s)

- Computers became common for businesses, governments, and the military.

- Data was now stored digitally → new risks appeared.
- **Main concerns:** unauthorized access, accidental loss of data, hardware failures.

Key Events:

- 1960s: U.S. military created ARPANET (early internet).
- 1970s: First known virus concepts (Creeper virus).
- 1980s: Personal computers spread, hackers started exploring vulnerabilities.

☞ Example: **Morris Worm (1988)** – one of the first major internet worms, caused thousands of computers to crash.

---

3. Modern Cybersecurity Era (1990s – Present)

- Internet became public → hackers, viruses, and cybercrimes exploded.
- New threats: phishing, ransomware, denial-of-service (DoS) attacks, identity theft.
- Companies started creating **firewalls, antivirus, intrusion detection systems (IDS)**.
- Governments introduced **cybersecurity laws** and standards.

Key Milestones:

- 2000s: Rise of **organized cybercrime** and state-sponsored attacks.
- 2010s: Cloud security, mobile device security, big data protection.
- 2020s: Focus on **AI, IoT, and ransomware defense**.

☞ Example: **WannaCry Ransomware (2017)** infected 200,000+ computers worldwide, shutting down hospitals, banks, and businesses.

Components of an Information System (IS)

An **Information System** is a structured setup that collects, processes, stores, and distributes information to support decision-making, coordination, control, analysis, and visualization in an organization.

It has **five main components**:

---

1. Hardware

- **Definition:** The physical devices used in an information system.
- Examples: computers, servers, routers, printers, storage devices, mobile phones.
- Role: Provides the **infrastructure** to process and store data.

☞ *Example :* The laptop you use in class, or the server in your college lab that stores assignments.

---

2. Software

- **Definition:** The programs and applications that run on hardware and process information.
- Types:
  - **System Software:** Operating systems (Windows, Linux, macOS).
  - **Application Software:** Word processors, accounting software, mobile apps.
- Role: Allows users and machines to **interact** with data.

☞ *Example :* MS Word (for assignments), Google Classroom (for submitting homework).

---

3. Data

- **Definition:** Raw facts and figures that are processed into meaningful information.
- Role: **Core of the system** – without data, no information system exists.
- Examples: Student grades, bank transactions, hospital patient records.

☞ *Example :* Your attendance records → raw data; Report Card → processed information.

---

4. People (Human Resources)

- **Definition:** Users who interact with the system and make decisions.
- Types of users:
  - **End users:** Students, employees, customers.
  - **IT professionals:** System admins, programmers, database managers.
- Role: People **use, manage, and protect** the system.

☞ *Example :* You (user), your teacher (admin), college IT staff (technical support).

---

5. Processes (Procedures/Policies)

- **Definition:** The methods, rules, and instructions that govern how the system works.
- Includes:
  - Security policies (password rules).
  - Data backup procedures.
  - Business rules (who can access what).
- Role: Ensures that the system works efficiently and securely.

☞ *Example :*
College rule: Only exam controller can upload final grades → this is a **process**.

Critical Characteristics of Information

For information to be **useful, reliable, and secure**, it must have certain **characteristics**. The most famous model is the **CIA Triad** (Confidentiality, Integrity, Availability), but there are more attributes too.

🔑 1. Confidentiality

- Ensures that **only authorized people** can access the information.
- Prevents **unauthorized disclosure** of data.

☞ Example for students:

- Your exam paper before the test must remain secret → only teachers can access it.
- If it gets leaked, confidentiality is broken.

Methods to protect confidentiality:

- Encryption, passwords, access control lists (ACLs).

🔑 2. Integrity

- Ensures that information is **accurate, correct, and unchanged** during storage or transfer.
- Prevents **unauthorized modification**.

☞ Example:

- If a hacker changes your grades from 75 to 95 in the database → integrity is lost.
- If bank account balance changes without transaction records → integrity is compromised.

Methods to protect integrity:

- Hashing, checksums, digital signatures, audit logs.

🔑 3. Availability

- Ensures that information and systems are **available when needed** by authorized users.
- Prevents **downtime** or denial of access.

☞ Example:

- If online exam servers crash during exams → availability is lost.
- If an ATM network is down, you cannot withdraw money.

Methods to ensure availability:

- Redundant systems, backups, disaster recovery plans, DDoS protection.

✨ Other Important Characteristics

4. Authenticity

- Verifies that the information and its source are **genuine and trustworthy**.
  ☞ Example: An official email from your university vs. a fake phishing email.

5. Accountability

- Tracks **who did what** in a system (through logs, monitoring).
  ☞ Example: If someone changes grades, logs should identify the person responsible.

6. Non-repudiation

- Ensures that a sender **cannot deny sending** a message or transaction.
  ☞ Example: When you transfer money online, a digital signature ensures you cannot later deny it.

7. Privacy

- Protects **personal or sensitive information** from being shared without consent.
  ☞ Example: Your medical records or student details must remain private.

Information Security Concepts and Practices

Information Security (InfoSec) is the **process of protecting information and information systems** from unauthorized access, misuse, disruption, or destruction.

At its heart, InfoSec is built on the **CIA Triad** (Confidentiality, Integrity, Availability) plus additional supporting practices.

🔑 1. The CIA Triad

a) Confidentiality

- Only **authorized people** can access data.
- Prevents data leakage or spying.
- Achieved by: **encryption, access controls, passwords, authentication systems**.

☞ Example:
Your email is protected with a password. If someone else reads it without permission, confidentiality is broken.

---

b) Integrity

- Information must be **accurate, complete, and unaltered**.
- Prevents **tampering** or accidental changes.
- Achieved by: **hashing, checksums, digital signatures, file permissions**.

☞ Example:
Banking system: If ₹1000 is transferred, records must show both debit (sender) and credit (receiver). If altered, integrity fails.

---

c) Availability

- Information and systems must be **available whenever needed** by authorized users.
- Prevents downtime and denial of access.
- Achieved by: **redundancy, backups, load balancing, DDoS protection, disaster recovery**.

☞ Example:
When you try to access an ATM, it should work 24/7. If the server crashes, availability is lost.

🔑 2. Other Key InfoSec Practices Beyond CIA

d) Authentication

- Verifies **who you are** before granting access.
- Methods: **passwords, biometrics (fingerprint, face scan), OTPs, smart cards**.

☞ Example:
When you log in to Facebook with username + password + OTP → multi-factor authentication.

---

e) Authorization

- After authentication, determines **what you can do**.
- Example: A student can view their marks, but only an admin can modify them.

---

f) Accountability

- Ensures actions can be **traced back** to users.
- Achieved with **audit logs, monitoring, CCTV, event tracking**.

☞ Example:
If someone changes exam results, the system logs show which user made the change.

---

g) Non-repudiation

- Prevents someone from **denying** their actions.
- Achieved by **digital signatures, transaction logs, blockchain**.

☞ Example:
When you pay via online banking, you cannot deny making the payment because records + signatures exist.

---

h) Privacy

- Protects **personal or sensitive data** from misuse.
- Controlled by **laws and policies** (e.g., GDPR, HIPAA).

☞ Example:
A hospital must keep patient medical records private.

🔑 3. Core Security Practices

Principles of Information Security:

1. **Least Privilege** – Give users only the access they need.
   ☞ Example: A cashier can access sales data, not HR salary details.
2. **Defense in Depth** – Use multiple layers of defense.
   ☞ Example: Firewall + antivirus + encryption + monitoring.
3. **Separation of Duties** – No single person should control all parts of a process.
   ☞ Example: In banks, one person approves a loan, another disburses it.
4. **Need-to-Know Principle** – Users access only what is required.
   ☞ Example: A student can access their own grades, not others'.

Types of Security Controls

- **Preventive Controls** → stop attacks (firewalls, encryption, access policies).
- **Detective Controls** → identify attacks (IDS, CCTV, system logs).

- **Corrective Controls** → fix damage (backups, patches, recovery plans).

🔑 4. Risk Management Concepts

- **Threat**: Potential danger (hackers, malware, natural disasters).
- **Vulnerability**: Weakness (weak passwords, unpatched systems).
- **Exploit**: When a threat uses a vulnerability to cause harm.
- **Risk**: Probability + impact of a threat exploiting a vulnerability.

☞ Example:

- Threat: Hacker
- Vulnerability: Weak Wi-Fi password
- Exploit: Hacker cracks Wi-Fi
- Risk: Data theft

Balancing Security and Access

🔑 1. What Does It Mean?

- **Security** = Protecting information and systems from unauthorized use.
- **Access** = Allowing authorized users to use information quickly and easily.
- **Balance** = Giving enough security to protect data, while still making it convenient for users.

☞ If security is **too strong** → users get frustrated.
☞ If security is **too weak** → hackers exploit the system.

🔑 2. The Dilemma

- Organizations must **protect information** but also **allow users to do their jobs**.
- Overly strict security can **slow down work**.
- Overly relaxed access can lead to **data breaches**.

🔑 3. Examples for Students

✓ Case 1: Passwords

- If you require a **20-character password** with special symbols, users may **write it down** → reduces security.
- If you allow **"12345"** as a password, hackers can break it easily.
- **Balanced approach**: Use 8–12 character strong passwords + two-factor authentication (2FA).

✓ Case 2: Online Banking

- Banks must protect accounts (security).
- Customers want to transfer money quickly (access).
- **Balanced approach**:
  - Require login + OTP for large transactions.
  - Allow easy balance checking without too many steps.

✓ Case 3: College Exam System

- Teachers must upload grades (access).
- Students must not see or edit them before release (security).
- **Balanced approach**:
  - Teachers log in with secure credentials.
  - Students can only view results after official release.

🔑 4. How to Achieve the Balance

- **Use Role-Based Access Control (RBAC):**
  Each user gets only the permissions needed (student, teacher, admin).
- **Apply Multi-Factor Authentication (MFA):**
  Strong login but still user-friendly.
- **Use Encryption Transparently:**
  Data is protected without users noticing extra steps.
- **Educate Users:**
  Train them about strong passwords, phishing, etc.
- **Continuous Monitoring:**
  Ensure balance remains effective as threats change.

How to Achieve the Balance Between Security and Access

---

1. Use Role-Based Access Control (RBAC)

- **Concept:** Each user gets **only the permissions** needed for their role, not more.
- This avoids both **excessive restrictions** (blocking normal work) and **excessive access** (security risk).

☞ **Example in College System:**

- **Students:** Can view their grades but cannot edit them.
- **Teachers:** Can upload/edit grades only for their subjects.
- **Admins:** Can manage the whole database.
- If a student had admin rights, they could change marks (security risk).
- If teachers were not allowed to upload grades online, it would delay results (usability issue).

✓ **Balanced Approach:** Assign roles properly → access is smooth + security is maintained.

---

2. Apply Multi-Factor Authentication (MFA)

- **Concept:** Requires **two or more ways** to verify identity (something you know, something you have, something you are).
- Makes logins **secure but still user-friendly**.

☞ **Example in Online Banking:**

- Login requires:
    1. Password (**something you know**)
    2. OTP sent to mobile (**something you have**)
- Even if a hacker steals your password, they cannot log in without your phone.

✓ **Balanced Approach:** Adds strong security without making it too hard (users just enter OTP).

---

3. Use Encryption Transparently

- **Concept:** Encrypt data automatically so users don't have to do extra steps.
- Protects information **without affecting usability**.

☞ **Example in Messaging Apps (like WhatsApp, Signal):**

- All chats are **end-to-end encrypted**.
- Users don't have to manually encrypt/decrypt → system does it automatically.
- This gives strong security (hackers cannot read messages) and easy access (users chat normally).

✓ **Balanced Approach:** Users enjoy security without extra burden.

---

4. Educate Users

- **Concept:** Users are often the **weakest link** in security (they click phishing emails, use weak passwords, etc.).
- Training helps them follow **safe practices** while still working efficiently.

☞ **Example in Office Environment:**

- If staff are trained not to click suspicious links → reduces phishing risk.
- If they understand password rules → they won't complain about "difficult" security.
- In a university, students can be taught about **safe Wi-Fi usage** and **avoiding fake websites**.

✓ **Balanced Approach:** Informed users follow security rules naturally, without slowing down their tasks.

---

5. Continuous Monitoring

- **Concept:** Security threats keep changing, so systems must be monitored **regularly**.
- Monitoring ensures the balance between security and usability is still effective.

☞ **Example in a Company Network:**

- If system logs show repeated failed logins → IT team may increase login security.

- If employees complain that security steps take too long → IT team may adjust policies.
- Cloud providers (like Google/AWS) continuously monitor servers to keep both speed (availability) and protection.

✅ **Balanced Approach:** Security is **updated as needed**, while access remains smooth.

Need for Information Security

Information is one of the **most valuable assets** for any individual, business, or government.
If information is stolen, changed, or destroyed, the results can be **financial loss, legal problems, damaged reputation, or even risks to human life**.

That's why **Information Security (InfoSec)** is essential.

✅ 1. Protection Against Cyber Threats

- The world is full of **hackers, malware, phishing scams, ransomware, and insider threats**.
- Without security, systems are easy targets.

👉 **Example:**
In 2017, the **WannaCry ransomware** attack affected 200,000+ computers worldwide, shutting down hospitals, banks, and transport systems.
Hospitals couldn't access patient data → lives were at risk.

✅ 2. Protecting Confidential Data

- Businesses and individuals handle **sensitive information** (personal details, financial records, exam results, trade secrets).
- If leaked, it can cause **privacy violations and identity theft**.

👉 **Example:**

- A university must protect student records from unauthorized access.
- A bank must secure account details to prevent fraud.

✅ 3. Ensuring Business Continuity

- Organizations depend on IT systems to function.
- If systems are attacked or go offline, operations stop → leading to **huge financial loss**.

☞ **Example:**
If an ATM network or e-payment system crashes due to a cyberattack, customers cannot withdraw money → business reputation is damaged.

✅ 4. Legal and Regulatory Requirements

- Many industries are required by **law** to secure information.
- Laws ensure that personal data is protected.

☞ **Examples of Regulations:**

- **GDPR (Europe):** Protects personal data and privacy.
- **HIPAA (USA):** Secures healthcare information.
- **ISO 27001:** International standard for information security management.
- Universities and banks in Nepal also have compliance rules.

Failure to follow these laws can result in **hefty fines and penalties**.

✅ 5. Maintaining Trust and Reputation

- Customers, employees, and partners trust organizations with their data.
- A single security breach can destroy that trust.

☞ **Example:**
When Facebook had data leaks (Cambridge Analytica scandal), users lost trust in the platform.
Many companies faced boycotts after breaches.

✅ 6. Protecting Intellectual Property

- Businesses invest in **research, designs, software, and strategies**.
- Hackers or competitors may try to steal this intellectual property.

☞ **Example:**
If a software company's source code gets leaked, competitors may copy it → huge financial loss.

✅ 7. National Security and Critical Infrastructure

- Governments must protect **military data, power grids, airports, hospitals, and financial systems**.
- Cyberattacks on such systems can cause **chaos or even war**.

☞ **Example:**
The **Stuxnet virus (2010)** targeted Iran's nuclear program → first major cyber weapon.