What Is Security?

Security is the condition of being **protected against threats, risks, or harm**.

Or

In general, **security** is "the quality or state of being secure—to be free from danger."

In the context of information systems, security ensures that **assets (especially information)** are safeguarded from unauthorized actions and misuse.

Security as a Concept

1. Security Is a Process, Not a Product

- Not a one-time installation
- Continuous and evolving
- Requires monitoring, improvement, and adaptation

2. Security Is a Non-Functional Requirement

- Does not perform business functions
- Ensures system functions operate safely
- Monitors violations of system properties

3. Security Is a Pervasive Concern

Security applies to:

- System design and architecture
- Applications and protocols
- Hardware and configurations
- Human behavior and awareness

Value of Information – Characteristics / Attributes

The value of information is derived from its **attributes**, which are tightly interconnected.

Availability

- Authorized users must access information when needed
- Information must be in the correct format
- Access should be uninterrupted

Accuracy

- Information must be correct and error-free
- Must meet end-user expectations

Authenticity

- Information must be genuine
- Ensures original creation
- Secure storage and transfer

Loss of authenticity reduces trust.

Confidentiality

- Prevents unauthorized disclosure

- Protects privacy and sensitive data

Integrity

- Information must remain whole and uncorrupted
- Any unauthorized change results in loss of integrity

Loss of authenticity, corruption, or destruction leads to integrity failure.

Utility

- Information must be useful
- Must be in a meaningful and usable format

Possession

- Ownership or control of information
- Losing possession does not always mean loss of confidentiality

Information security

Information Security (InfoSec) is the practice of **protecting information and information systems** from **unauthorized access, use, disclosure, disruption, modification, or destruction**.

Evolution from Computer Security to Information Security

Computer Security (Early Focus)

Initially, security focused only on **computers and hardware**.

Key characteristics:

- Protection of mainframe computers
- Physical access control
- Limited number of users

Security was mainly about **protecting machines**, not data.

Transition to Information Security

As technology evolved:

- Data became more valuable than hardware
- Networks connected multiple systems
- Information began flowing outside physical boundaries

Security focus shifted from **machines → information**.

Thus, **Information Security** emerged as a broader discipline.

Why Information Security is Needed

Information security is required to:

- Protect sensitive information
- Prevent unauthorized access and misuse
- Ensure business continuity
- Maintain trust and compliance

Threats include:

- Cyberattacks
- Insider threats
- Human error
- System failures

Core Principles of Information Security – CIA Triad

The **CIA Triad** is the foundation of Information Security. It defines **what we must protect** in any system or data.

CIA stands for:

C – Confidentiality

I – Integrity

A – Availability

1. Confidentiality 🔐

Definition

Confidentiality ensures that **information is accessible only to authorized users** and not disclosed to unauthorized individuals.

Why it matters

- Prevents data leaks
- Protects personal, financial, and sensitive business data

How Confidentiality is Achieved

- **Authentication** – username, password, biometrics
- **Authorization** – role-based access (RBAC)
- **Encryption** – AES, RSA, HTTPS
- **Data masking** – hiding sensitive fields
- **Access control lists (ACLs)**

Real-World Examples

- Bank account details visible only to the account holder
- HTTPS encrypting data between browser and server
- Company files accessible only to employees

Violation Example

- Data breach exposing user passwords

2. Integrity 🛡️

Definition

Integrity ensures that **data remains accurate, complete, and unaltered** unless modified by authorized users.

Why it matters

- Prevents unauthorized changes
- Ensures trust in data and systems

How Integrity is Achieved

- **Hashing** – SHA-256

- **Digital signatures**
- **Checksums**
- **Database constraints**
- **Version control systems (Git)**

Real-World Examples

- Git commit hash detects code changes
- Digital signatures in software downloads
- Hash verification while downloading files

Violation Example

- Hacker modifies transaction amount in a database

3. Availability ⚙️

Definition

Availability ensures that **systems, services, and data are accessible when needed** by authorized users.

Why it matters

- Business continuity
- User trust
- Prevents service downtime

How Availability is Achieved

- **Redundancy** – multiple servers
- **Load balancing**
- **Backups**
- **Disaster recovery plans**
- **DDoS protection**
- **Auto-scaling (Cloud)**

Real-World Examples

- Google services always available
- ATM working 24/7
- Cloud failover systems

Violation Example

- DDoS attack bringing a website down

Building the CIA Triad

The CIA triad cannot be achieved by technology alone.

It requires a combination of:

Security Policies

High-level statements defining security goals and responsibilities.

Procedures

Step-by-step instructions to implement policies.

Guidelines

Recommended practices that are flexible.

Standards

Mandatory rules and baselines.

People, Process, and Technology (PPT Model)
Effective information security must address **all three components**.
People

- Users, employees, administrators
- Must follow security policies
- Often the **weakest link** in security

Kevin Mitnick emphasized that even the best technology fails if people make mistakes.

Process

- Defined methods for handling information
- Includes procedures, workflows, and controls
- Implemented using technology and followed by people

Technology

- Tools used to enforce security
- Includes hardware, software, and systems

Technology supports people and processes but cannot replace them.

History and Evolution of Information Security
Early Days – Computer Security

- Emerged after development of mainframe computers
- Influenced by World War II code-breaking efforts

Initial focus:

- Physical protection of computers
- Restricted access to memory and machines

Enigma Machine

- German encryption machine used during World War II
- Used for sending coded military messages
- Highlighted importance of information secrecy

ARPANET and Network Security

- Developed by Advanced Research Project Agency (ARPA)
- Led by Larry Roberts
- Focused on:
    - Redundant communication
    - Networking and resource sharing

Security problems:

- No authentication
- No authorization
- Insecure dial-up connections

RAND Report (R-609)

- First formal report on computer security
- Expanded security focus to include:
    - Data protection
    - Limiting unauthorized access
    - Personnel roles and authorization levels

Key realization:

- Data could be stolen **without physical access** to computers

1990s and the Internet Era

- Rapid growth of computer networks
- Birth of the global Internet

Security challenges:

- Security was a low priority
- Lack of awareness about risks
- Sensitive information shared openly

Types of Information - 5 types

Information Security is divided into multiple types based on **what is being protected** and **where the threat exists**. Each type focuses on a different layer of an organization's IT environment.

1. Network Security 🌐

What it is

Network Security protects data and systems **while data is traveling over networks** (internal or internet).

What it protects

- Network traffic
- Servers and network devices
- Internal communication between systems

Common Threats

- Unauthorized access
- DDoS attacks
- Man-in-the-Middle (MITM)
- Packet sniffing

Security Mechanisms

- **Firewalls** – filter incoming and outgoing traffic
- **IDS (Intrusion Detection System)** – detects attacks
- **IPS (Intrusion Prevention System)** – blocks attacks
- **VPN (Virtual Private Network)** – secure remote access
- **Network segmentation** – isolate critical systems

Real-World Example

- Corporate VPN for work-from-home employees
- Firewall blocking suspicious IP addresses

3. Data Security 💾

What it is

Data Security protects **data itself**, regardless of where it is stored or used.

Data States

- Data at rest
- Data in transit
- Data in use

Common Threats

- Data theft
- Data leakage
- Unauthorized modification

Security Mechanisms

- Encryption (AES, RSA)
- Tokenization
- Data Loss Prevention (DLP)
- Database access controls
- Backups

Real-World Example

- Encrypting database passwords
- HTTPS protecting API data

4. Endpoint Security 🖥️

What it is

Endpoint Security protects **end-user devices** that connect to the network.

Endpoints Include

- Laptops
- Desktops
- Mobile devices
- Tablets

Common Threats

- Malware
- Ransomware
- USB attacks
- Phishing

Security Mechanisms

- Antivirus & Anti-malware
- EDR (Endpoint Detection & Response)
- Disk encryption (BitLocker)
- Device control policies
- OS patching

Real-World Example

- Antivirus on employee laptops
- Blocking unauthorized USB devices

5. Cloud Security
What it is
Cloud Security focuses on securing **data, applications, and infrastructure hosted in the cloud**.
Shared Responsibility Model
- Cloud provider: physical infrastructure
- Customer: data, access, configurations

Common Threats
- Misconfigured storage (public S3 buckets)
- Identity theft
- Insecure APIs

Security Mechanisms
- IAM (Identity & Access Management)
- Encryption
- Cloud firewalls
- Security groups
- Monitoring & logging

Real-World Example
- AWS IAM roles for least privilege
- Securing cloud databases

Information Security Management System (ISMS)
An **Information Security Management System (ISMS)** is a **systematic, documented, and continuous approach** to managing sensitive information so that it remains **secure**. It combines **people, processes, and technology** to protect information assets and manage security risks.

In simple words:
ISMS is a **management framework** that helps an organization **identify security risks and apply controls** to protect information.

Why ISMS is Needed
Organizations today face:
- Data breaches
- Cyberattacks
- Insider threats
- Legal & compliance requirements

ISMS helps to:
- Protect confidential data
- Reduce security risks

- Ensure business continuity
- Meet legal and regulatory compliance
- Build customer trust

Objectives of ISMS

The main objectives of ISMS are to:

- Ensure **Confidentiality, Integrity, and Availability (CIA)**
- Identify and manage information security risks
- Establish clear security policies and procedures
- Continuously improve security posture

Key Components of ISMS

People

- Employees
- Management
- Security teams

Role:

- Follow security policies
- Receive security awareness training
- Report incidents

Processes

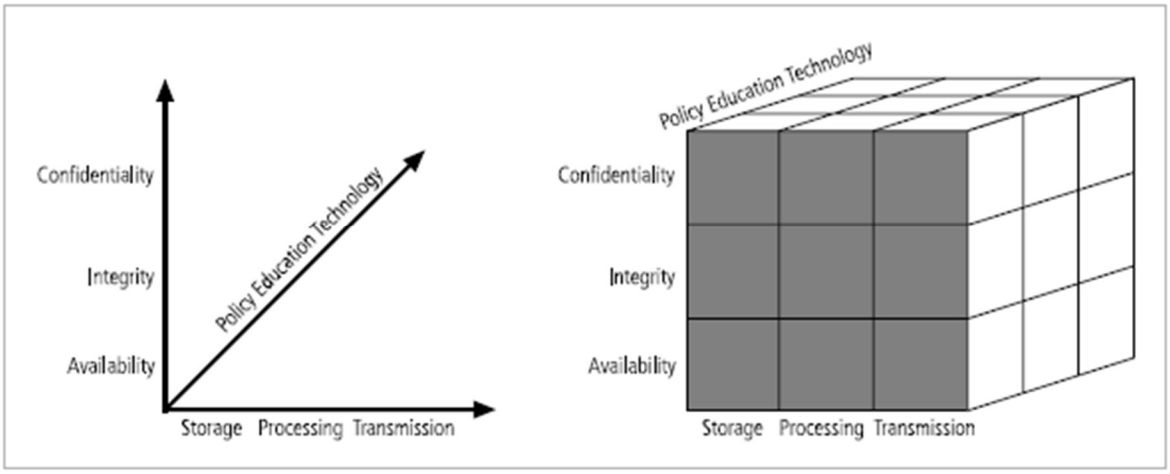
- Risk assessment
- Incident response
- Access management
- Change management
- Audit and compliance

Technology

- Firewalls
- Encryption
- IAM systems
- Antivirus / EDR
- SIEM tools

CNSS Security Model

The CNSS Security Model (McCumber Cube) is a three-dimensional framework that integrates security objectives, information states, and security measures to comprehensively secure information systems.



Components of an Information System (IS)

An **Information System (IS)** is not limited to computers alone. It is a complete set of interrelated components that work together to **collect, process, store, and distribute information** in an organization. An IS consists of **six critical components**:

1. Software
2. Hardware
3. Data
4. People
5. Procedures
6. Networks

Each component has **unique characteristics, strengths, weaknesses, and security requirements**.

1. Software

Software includes:

- Application software
- Operating systems
- Utility and command programs

Importance

- Software carries and processes organizational information.
- It controls how data is accessed, processed, and stored.

Security Issues

- Software is **the most difficult IS component to secure**.
- Programming errors (bugs, loopholes, vulnerabilities) are a major cause of cyberattacks.
- Many attacks exploit flaws in poorly written or poorly tested software.

Key Problems

- Software is often developed under constraints of **time, cost, and manpower**.
- Security is frequently added **after development**, not during design.
- This makes software an **easy target** for accidental or intentional attacks.

Example

- Crashing smartphones

- Faulty automotive control software leading to vehicle recalls

2. Hardware

Hardware refers to the **physical devices** used in an information system, such as:

- Computers and servers
- Storage devices
- Input/output devices
- Networking equipment

Importance

- Hardware houses software and data.
- It provides physical interfaces for information entry and output.

Security Issues

- Physical access to hardware can lead to **data theft or destruction**.
- If attackers gain unrestricted access to hardware, information security **cannot be guaranteed**.

Physical Security Measures

- Locks and keys
- Restricted access areas
- Surveillance and monitoring

Example

- Laptop theft in public places (airports)
- Value of stolen data is often **much higher** than the cost of the device

3. Data

Data is the information that is:

- Stored
- Processed
- Transmitted by the system

Importance

- Data is often the **most valuable asset** of an organization.
- It is the **primary target** of most attacks.

Security Issues

- Improper database configuration reduces security.
- Many systems fail to fully use **database management system (DBMS) security features**.
- Poor implementation may be less secure than traditional file systems.

Key Point

- Protecting data confidentiality, integrity, and availability is critical.

4. People

People include:

- Employees
- Users
- Administrators
- Managers
- External users

Importance

- People interact with all components of the IS.
- They can protect or compromise system security.

Security Issues

- Humans are often the **weakest link** in information security.
- Errors, negligence, or malicious intent can lead to security breaches.

Social Engineering

- Attackers manipulate people into revealing confidential information.
- Exploits trust, carelessness, or lack of awareness.

Example

- Bribing a gatekeeper instead of breaking a wall (historical analogy)

Solution

- Security policies
- Education and training
- Awareness programs
- Proper use of technology

5. Procedures

Procedures are:

- Written instructions for performing tasks
- Guidelines for using information systems

Importance

- Procedures define how systems are operated securely.
- They are **information assets themselves**.

Security Issues

- Unauthorized access to procedures can compromise system integrity.
- Poorly protected procedures can lead to major financial losses.

Example

- Bank consultant used internal procedures to illegally transfer millions of dollars due to weak authentication.

Key Point

- Procedures should be shared on a **need-to-know basis**.
- Employees must be trained to **protect procedural information**.

6. Networks

Networks connect:

- Computers within an organization (LAN)
- Organizations to external systems (Internet)

Importance

- Networking enables data sharing and communication.
- It increases efficiency and accessibility.

Security Issues

- Networking introduces **new and complex security challenges**.
- Physical security alone is not sufficient in networked environments.

Network Security Measures

- Firewalls
- Intrusion detection and prevention systems
- Monitoring and alarms
- Access control mechanisms

Key Point

- Networks are the main reason for the **increased need for information security** today.

Characteristics of Good IT Security

Good IT security should be:

1. **Effective**
    - Performs its intended security function.
2. **Efficient**
    - Easy to operate and manage.
3. **Economical**
    - Cost-effective and affordable.
4. **Accepted / Unobtrusive**
    - Users should not feel overly restricted or annoyed.

Reality Check: No System Is 100% Secure

- New threats and vulnerabilities appear continuously.
- Absolute security is **impossible**.
- Security is about **risk management**, not total elimination of risk.

Balancing Security vs. Access

- More security → Less convenience
- More convenience → Less security

This creates a constant conflict:

- **CISO** wants maximum security
- **Users** want quick and easy access

A balance must be achieved between:

- Protection
- Usability
- Availability

The "Seven I's" and "Five Categories" of Security

Seven I's:

1. Confidentiality
2. Integrity
3. Availability
4. Reliability
5. Compliance

6. Effectiveness
7. Efficiency

Five Categories:

1. Application
2. Technology
3. Facilities
4. Data
5. People

Each of the **seven I's** must be applied to **all five categories** for comprehensive security.

Issues and threats in information security -CIA triad

CONFIDENTIALITY

Confidentiality (also called **privacy**) means:
Protecting information from unauthorized disclosure.
Only authorized individuals should be able to access sensitive information.

Key Questions to Define Confidentiality

1. **What needs protection?**
    - Personal information
    - Privileged data
    - Business secrets
    - Geological or environmental data
2. **How much protection is required?**
    - Depends on sensitivity level.
3. **For how long should protection be maintained?**
    - Temporary?
    - Permanent?
    - Until business value expires?

Examples Highlighted

Example 1: Geological Data Exploit

A criminal uses geological information to dig a tunnel to a bank's safety vault.
Shows that even non-traditional data can be sensitive.

Example 2: Earthquake Simulation Attack

Criminals simulate an earthquake to bypass security systems in a data center.
Demonstrates indirect attacks on confidentiality.

Threats to Confidentiality

1. Hackers

Unauthorized users attempting to steal information.

2. Masquerading

An attacker pretends to be an authorized user.

3. Unauthorized User Activity

Authorized users performing actions beyond their privileges.

4. Malware in Downloaded Files

Opening infected files can expose sensitive data.

5. LAN Vulnerabilities

Local networks are initial exposure points for attacks.

6. Trojan Horses

Backdoors installed to steal data.

Example:

A database system had a hidden admin login:

- Username: politically
- Password: correct
  This vulnerability remained hidden for 7 years.

INTEGRITY

Definition

Integrity refers to:

The trustworthiness, correctness, and reliability of data.

Data must:

- Be accurate
- Come from a trusted source
- Remain unaltered unless authorized
- Maintain correct format

Main Challenge

Data must remain:

- In expected state
- In expected format
- Accessible only to authorized individuals
- Free from intentional or accidental modification

PRINCIPLES OF INTEGRITY

1. Need-to-Know Principle

Users access only information necessary for their tasks.

2. Need-to-Do Principle

Users perform only actions required for their roles.

3. Segregation of Duties (Separation of Duties)

Divide responsibilities among multiple individuals.

Example:

- System Admin → Creates user account
- User → Sets password

No single person has full control.

4. Rotation of Duties

Frequently changing personnel handling tasks.

Purpose:

- Prevents single point of failure
- Avoids exclusive knowledge
- Detects hidden manipulation
- Introduces redundancy

If only one person understands a system, they could manipulate it without detection.

INTERNAL THREATS TO INTEGRITY

🔹 **1. Disgruntled Employee**

Modifies hidden system parameters that activate later, causing crashes.
Hard to trace.

🔹 **2. Accidental Event (NYSE Example)**

Attempt to sell massive stocks → Server crash
Caused:

- Integrity issues
- Availability problems

🔹 **3. Logic Bomb**

Malicious code triggered under specific condition.
Example:
Delete all server files if employee name removed from payroll.

AVAILABILITY

🔹 **Definition**

Availability means:
Information and system services must be accessible to authorized users when needed, without undue delay.

Dual Nature of Availability

1. Ensure authorized access
2. Prevent denial-of-service attacks

DENIAL OF SERVICE (DoS)

🔹 **Definition**

An attack that prevents legitimate users from accessing resources.

🔹 **Example: Network Choking**

Attacker floods network with fake packets.
Effects:

- Network congestion
- Device overload
- Slow legitimate communication
- Service disruption

INFORMATION SECURITY CONTROLS

To maintain CIA, organizations must implement **controls**.

Why Controls Are Necessary

1. Organizational survival
2. Prevent costly data loss
3. Avoid system downtime
4. Ensure correct decision-making
5. Protect from hacking and viruses
6. Prevent destruction and theft
7. Prevent unauthorized use
8. Avoid physical damage to systems

TYPES OF CONTROLS

Administrative Controls

Defined through:

- Policies
- Procedures
- Organizational structure
- Security guidelines

They define:

- What is allowed
- What is prohibited

Example:

- Password policy
- Data classification policy
- Access management policy

Technical Controls

Technical mechanisms that enforce policies.

Examples:

- Firewalls
- Encryption
- Authentication systems
- Intrusion Detection Systems
- Access Control Lists

They actively prevent:

- Disclosure
- Alteration
- Destruction

NEGATION OF CIA (DAC Model)

Opposites of CIA:

CIA Goal	Opposite Threat
Confidentiality	Disclosure
Integrity	Alteration
Availability	Destruction

Controls protect against:

- Unauthorized disclosure
- Unauthorized alteration
- Destruction of resources

CONTROL MECHANISMS FOR INFORMATION SECURITY

Introduction

Information Security Control Mechanisms are implemented to ensure the three core objectives of security:

- **Confidentiality**
- **Integrity**
- **Availability (CIA)**

Without proper controls, organizations face:

- Data loss
- Fraud
- System crashes
- Incorrect business decisions
- Organizational collapse

Rotation of Duties

- **Definition**

Rotation of duties ensures that:

The same person is not responsible for maintaining an activity for too long.

Purpose

- Prevents one individual from having exclusive control
- Avoids “data ownership monopoly”
- Creates redundancy
- Ensures multiple people understand critical systems
- Detects hidden manipulation

Problem It Solves

If only one person:

- Knows how a system works
- Controls specific data
- Maintains certain configurations

That person can:

- Manipulate data
- Introduce malicious code
- Hide fraud

Rotation reduces single-point-of-failure risk.

Consequences of No Control

1. Data loss
2. Operational errors
3. Denial of service
4. Wrong business decisions
5. Internal fraud
6. External hacking
7. Theft of information assets
8. System destruction
9. Operational disruption
10. Physical damage

Definition of Control (COBIT Perspective)

Control consists of:

- Policies
- Procedures
- Practices
- Organizational structures

🔹 **Objective of Control**

To provide:

Reasonable assurance that business objectives are achieved and undesired events are prevented, detected, and corrected.

Types of Internal Controls

1. Preventive Controls

Stop incidents before they occur.

Examples:

- Antivirus blocking malware
- Firewalls
- Access restrictions

2. Detective Controls

Identify incidents after they occur.

Examples:

- Intrusion detection systems
- Audit logs

- Antivirus detection alerts

3. Corrective Controls
Fix damage after detection.
Examples:
- Removing malware
- Restoring backup
- Patching systems

General Controls (11 Key Areas)
1. Security Plan
Comprehensive coverage of:
- Physical security
- Hardware
- Software
- People
- Process
- Technology

2. Segregation of Duties
Different individuals perform critical tasks.

3. Project Development Controls
Security integrated during system development.
Example:
Confidential handling of Aadhaar data.

4. Physical Access Controls
Control building/data center entry.

5. Logical Access Controls
Control digital access (passwords, authentication).

6. Data Storage Controls
Define:
- Backup
- Storage format
- Access rights

7. Data Transmission Controls
Secure communication between systems.
Examples:
- VPN
- SAN

- NAS

8. Documentation Standards
Ensures:
- Transparency
- Auditability
- Fraud prevention

9. Minimize System Downtime
Important for availability.

10. Disaster Recovery Plans
Plan for:
- Data migration
- System restoration
- Emergency continuity

11. Protection of PCs & Networks
Prevents:
- Individual compromised clients
- Internal DoS
- Malware spread

Internet Control
When connecting internal systems to internet:
Risks increase significantly.
Requires:
- Strong firewalls
- Network monitoring
- Strict policies
- Access restrictions