

Data Privacy and Information Security

By:- Er.Ranjeet Ranjan

A. Data Privacy

- Data privacy concerns how personal information is collected, used, shared, retained and deleted.

Example: A government office collects Aadhaar for legal purposes; must ensure it's not shared unnecessarily.

B. Information Security

- Protects information from unauthorized access, alteration, disclosure, destruction or disruption.

Example: An officer uses a strong password, MFA and access controls to protect a welfare database.

C. Cybersecurity

- Protects computers, networks, applications, digital accounts and data against cyberattacks.

Example: Preventing ransomware from encrypting a district office's computer systems.







Concept	Main question	Government example
Data privacy	Should this information be collected, used or shared?	Should an applicant's phone number be disclosed to another department?
Information security	How do we protect the information?	Who can access the applicant database?
Cybersecurity	How do we protect digital systems from attacks?	How do we prevent phishing and ransomware?

The Three Pillars of Information Security: CIA Triad

C — Confidentiality

- Only authorized persons can access information.

Example: Only authorized officials can view confidential investigation records.

I — Integrity

- Information remains accurate, complete & protected from unauthorized modification.

Example: A beneficiary's approved pension amount cannot be changed by an unauthorized user.

A — Availability

- Information and services remain accessible to authorized users when required.

Example: A district hospital can access authorized digital records during emergencies.

Classroom question: If a cyberattack changes pension amounts, which pillar is affected?

Answer: Integrity. If it exposes citizens' records, confidentiality is affected. If it disables the system, availability is affected. One incident can affect all three.

Types of Data Handled

Type of information	Examples	Appropriate handling
Public information	Published government schemes, public notices	Share through authorized public channels
Personal data	Name, phone number, address, bank details	Use only for authorized purposes & protect against unauthorized disclosure
Sensitive operational info	Investigation details, security arrangements, credentials	Restrict access according to official authorization
Confidential administrative	Unpublished decisions, personnel files, internal correspondence	Follow applicable classification and access rules
Authentication info	Passwords, OTPs, recovery codes, private keys	**Never disclose to others or place in public documents**

Practical Example: A District Welfare Office

Scenario: Imagine that a district office maintains a database containing names, addresses, bank details and pension status of 20,000 beneficiaries.

Ask the trainees:

- Should every employee be allowed to download the entire database?
- Should the list be forwarded to a personal email account to complete work at home?
- Can the full list be posted in a public WhatsApp group to verify beneficiaries?
- What should an officer do if the list is accidentally sent to the wrong recipient?

Expected answer: Access must be limited to authorized work requirements, approved systems used, unnecessary disclosure avoided, and accidental exposures reported promptly through official channels.

Data Privacy Principles Must Follow

1. Purpose limitation

Collect and use for specified, lawful purpose. Do not reuse for unrelated personal/admin tasks without authority.

2. Data Minimisation

Collect only what is necessary. If a service does not require full bank statements, do not demand or retain them.

3. Accuracy

Maintain accurate records. Incorrect beneficiary details cause wrongful rejection or misdirected payments.

4. Storage limitation

Keep data only as long as required by records-retention schedules. Do not destroy legally preserved records.

5. Controlled sharing

Verify recipient, authority and purpose before sharing information with another department or vendor.

6. Accountability

Maintain appropriate approvals, access logs and records of data decisions so misuse can be investigated.

Information Security Threats & Real-Life Defences

A. Phishing: Fraudulent emails/messages imitating departments to steal credentials or inject attachments.

Example: Account suspension warning link. | **Defence:** Verify sender independently; never click suspicious links.

B. Ransomware: Malicious software encrypts data/disrupts systems with extortion demands.

Example: District office losing land records. | **Defence:** Protected offline backups, software patches, endpoint controls.

C. Social Engineering: Attackers manipulate staff to bypass established security gates.

Example: Caller claiming to be senior officer demanding OTP. | **Defence:** Verify via official channel; never disclose OTPs.

D. Removable-Media & Device Risks: Unknown USBs, unpatched machines, or lost laptops exposing files.

Example: Copying beneficiary files to personal USB. | **Defence:** Use authorized, encrypted devices; adhere to device policies.

E. Accidental Disclosure & Insider Misuse: Employees exposing data through errors or intentional misuse.

Example: Uploading spreadsheets to public sites. | **Defence:** Verify recipients, restrict permissions, audit sharing logs.











Legal and Regulatory Framework in India

Law, rule or framework	Relevance to officers
Digital Personal Data Protection Act, 2023	Framework for processing digital personal data, individual rights & fiduciary duties
Digital Personal Data Protection Rules, 2025	Rules concerning implementation of the DPDP framework
Information Technology Act, 2000	Legal provisions relating to electronic records, cyber offences and security
CERT-In Directions, 2022	Mandatory cyber incident reporting and specified cybersecurity requirements
CERT-In Guidelines on Info Security (2023)	Government-focused information security controls and operational practices
Right to Information Act, 2005	Public access to information, subject to exemptions & legal limits
Departmental rules and records policies	Official access, retention, disclosure, security classification and reporting

A. Digital Personal Data Protection Act, 2023

Data Principal: Individual to whom the personal data relates.

Personal Data: Data about identifiable individual.

Security Safeguards: Mandatory safeguards as legally provided.

Data Fiduciary: Entity determining purpose & means of processing.

Consent & Lawful Processing: Permitted basis; consent isn't sole ground.

Breach Response: Mandated notifications upon personal data breach.

B, C & D. IT Act, CERT-In & RTI Act, 2005

B. IT Act, 2000

Sec 43: Unauthorized system & data access.

Sec 66: Dishonest computer-related acts.

Sec 66C: Identity theft & fake e-signatures.

Sec 66D: Personation cheating using computers.

Sec 70B: CERT-In incident response powers.

C. CERT-In Reporting

2022 Directions: Mandates specified entities to report listed cyber incidents within 6 hours of noticing them.

Prescribes log retention and organizational external reporting obligations beyond internal chains.

D. RTI Act, 2005

Distinguish transparency from indiscriminate disclosure. Assess protected material under exemptions and public interest.

Trainer note: Privacy is no blanket excuse to deny info, and transparency is not permission to leak personal data.

Practical InfoSec Measures for Government Offices

1. Password & Authentication

Long unique passphrases • MFA enabled • Never share OTPs/passwords • Reject unexpected authentications • Use approved managers.

2. Computer & Network

Install security updates promptly • Lock desk computer • Use approved endpoint tools • Do not connect personal devices to govt nets.

3. Backup & Recovery

Maintain departmental backups • Protect from ransomware • Store in approved separated sites • Periodic restoration tests • Continuity plan.

4. Physical & Document

Secure confidential paper files • Clear unattended printouts • Verify identity before release • Sanitize disposals • Report lost devices.









Safe Handling of Email, WhatsApp and Digital Documents

Situation	Unsafe practice	Safer practice
Receiving urgent email	Clicking immediately	Verify sender and request through independent channel
Sending beneficiary list	Sending full spreadsheet to everyone	Share only authorized, necessary info with approved recipients
Working from home	Forwarding official records to personal email	Use approved remote-access and document-sharing systems
Sharing a file	Making public link accessible to anyone	Restrict access to authorized recipients and set permissions
Receiving an OTP request	Sharing OTP with a caller	Refuse and verify the caller's identity
Using WhatsApp	Sharing confidential files in unofficial group	Follow departmental policy & use approved channels
Discarding an old laptop	Giving it away with files intact	Follow approved sanitization and disposal procedures

Important distinction: Encrypted messaging apps do not make unauthorized data sharing lawful. Recipient, purpose, departmental rules and data sensitivity still matter.

Classroom Exercise: Identify the Phishing Email

[SIMULATED TRAINING EXAMPLE]

Subject: URGENT — Government Email Account Will Be Blocked Today

Sender: IT Support

"Dear Officer, Your official email account will be suspended within 30 minutes due to a security violation. Click the verification link below and enter your password and OTP to avoid suspension."

Verify your account immediately

Ask Trainees: Warning Signs Identified

- **Artificial urgency:** Threat of 30-minute account suspension.
- **Sensitive disclosure request:** Direct demand for password & OTP.
- **Unverified sender:** Display identity differs from authorized domain.
- Safe because it uses official tone**False trap:** Attackers always mimic official administrative language.

Data Breach: Incident-Response Procedure

Step 1 — Recognize and report

Notify designated IT/security team, reporting officer, or response channel immediately. Do not wait for full scope.

Step 2 — Contain the incident

Follow instructions to isolate devices/accounts and revoke sessions. Never improvise actions damaging evidence.

Step 3 — Preserve evidence

Record time, systems, messages, actions. Preserve logs. Do not wipe devices or delete messages unless instructed.

Step 4 — Recover securely

Technical team investigates cause, purges threats, restores from clean backup, and validates safeguards.

Step 5 — Meet reporting and notification requirements

Assess CERT-In (6-hr) and DPDP breach notifications. Document actions taken and corrective systemic safeguards.

Accidental Disclosure of Pension Data

Scenario & Discussion:

An officer emails an Excel file with names, bank accounts, and phone numbers of 5,000 beneficiaries to an external recipient instead of a colleague.

- Harms to citizens?
- Officer's first 15-minute response?
- Who must be informed?
- Does recalling/deleting the email solve the problem?
- Long-term preventive safeguards?

Suggested Trainer Answer:

- Report disclosure immediately through incident chain.
- Inform supervisory team & data-protection function.
- Preserve audit trail of sent messages.
- Request external recipient deletion (does not eliminate incident).
- Assess breach notifications and implement data minimisation.

Key message: Honest mistakes must be reported promptly; concealing escalates harm.

Data Privacy and AI Tools in Administration

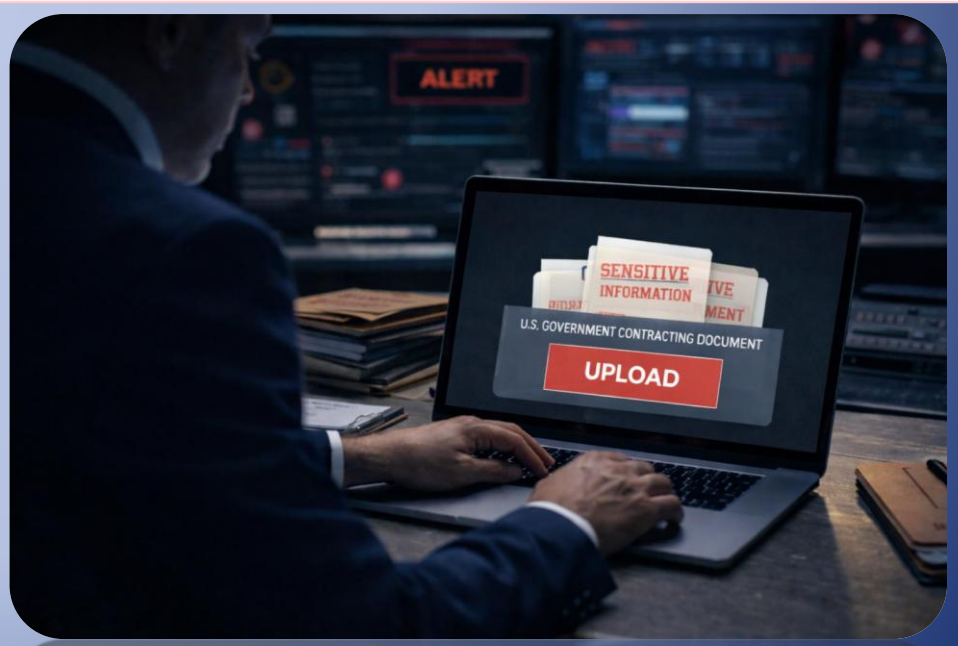
Safe Use of AI

- Drafting general circulars using fictional or public data.
- Explaining laws or summarising public policy documents.
- Using anonymised/synthetic data for training exercises.
- Verifying AI legal, financial & administrative outputs before official use.



Unsafe Use of AI

- Uploading Aadhaar numbers, bank details or case files into unapproved AI tools.
- Uploading confidential investigations or unpublished policies.
- Pasting passwords, API keys or access tokens into prompts.
- Making decisions on citizens without human review & legal authority.



Classroom Exercise: Which Prompt is Safer?

SAFER APPROACH

“Draft a standard pension verification letter using fictional beneficiary details. Include a checklist of documents an officer should verify under the applicable scheme rules.”

Avoids exposing actual personal data while completing administrative work.

UNSAFE WITHOUT AUTHORIZATION

“Here is our complete pension database with names, Aadhaar numbers, bank accounts and mobile numbers. Identify suspicious beneficiaries.”

Massive data breach risk: actual identifiable data leaked to public LLMs.

Practical Group Activities for Officer Trainees

Activity 1 — Data Classification

Classify: Published guidelines, Beneficiary bank list, Disciplinary file, Press release, Employee credentials.

Learning: Classification dictates handling; credentials never public.

Activity 2 — Senior Officer's Request

Unknown WhatsApp number claims to be senior officer demanding immediate database transfer.

Learning: Independent verification, authorized transfers, report impersonation.

Activity 3 — District Office Audit

Act as inspection team evaluating passwords, records, patches, backups, staff awareness & continuity plans.

Learning: Cyber hygiene is administrative, not purely IT's job.

Officer Training Quiz (Questions 1–3)

1. What is the primary objective of data privacy?

- **Correct:** To ensure personal data is handled appropriately and lawfully.

(Incorrect: To prevent all data collection / To keep every government record secret)

2. Which is NOT one of the CIA Triad principles?

- **Correct:** Convenience.

(Principles are: Confidentiality, Integrity, Availability)

3. An unknown caller requests an OTP for urgent official work. What should the officer do?

- **Correct:** Refuse and verify the request independently.

(Incorrect: Share if caller knows designation / Send OTP to colleague)

Officer Training Quiz (Questions 4–6)

4. What is the correct first response to a suspected data breach?

- **Correct:** Report promptly through the official incident-response channel.

(Incorrect: Delete all evidence / Wait until full investigation completes)

5. Can an officer upload an identifiable beneficiary database to any AI tool?

- **Correct:** Only when authorized under applicable rules and approved safeguards.

(Incorrect: Yes if it saves time / Yes if file is in Excel format)

6. What does data minimisation mean?

- **Correct:** Collect only data necessary for the legitimate purpose.

(Incorrect: Delete all records every month / Make all data anonymous when ID legally required)

Official Resources for Further Reading

CERT-In Guidelines
Security controls, email/phishing guidance, removable media, incident reporting & government-focused practices.

MeitY DPDP Portal
Consult notified legislation, rules, corrigenda and commencement notifications before teaching legal obligations.

India Code
Use authoritative statutory text to prepare the legal-framework portion of the class.

• CONCLUDING MESSAGE

“Data privacy and information security are not merely technical responsibilities; they are essential duties of public administration. Every citizen who submits a form, applies for a welfare scheme or shares personal information with a government office places trust in that institution. As officers, we must protect that trust by collecting only what is necessary, using information responsibly, restricting unauthorized access and responding promptly when something goes wrong. A secure government is not only a government with strong technology; it is a government with responsible, accountable and security-conscious officers.”