



MODULE 4

Cyber Security, Data Protection and Digital Ethics

Protecting sensitive complaint information while sustaining trust, lawful processing and resilient digital operations.

Theme: Strengthening Ombudsman Service Delivery through Digital Transformation, Artificial Intelligence and Electronic Complaint Management

By the end, participants can identify cyber risks, apply data-protection practices and respond to incidents responsibly.

Why security is central to digital service delivery

Public confidence depends on confidentiality, integrity and responsible information handling.

Complaint records may contain personal, sensitive and reputationally significant information.

Digital systems increase access but also increase exposure to cyber threats. Security failures can disrupt investigations and damage institutional credibility. Every officer has a role in protecting information and reporting incidents.

Trust is a service-delivery asset; protect it daily.



Secure complaint information management

Information security

Protecting information from unauthorised access, alteration, disclosure or disruption.

Confidentiality: only authorised persons can access sensitive information.

Integrity: information remains accurate, complete and unaltered.

Availability: authorised users can access systems when needed.

Security combines policies, behaviour, technology and leadership oversight.

Information security begins before a breach occurs.



Secure complaint information management

Core cyber security principles

Cyber security protects systems, networks, software and electronic information.

Confidentiality

Protect information from unauthorised disclosure.

Integrity

Prevent unauthorised alteration or corruption.

Availability

Ensure systems and records remain usable.

Authentication

Verify user identity before access.

Accountability

Record actions and enforce responsibility.

Risk management

Identify, reduce and monitor risks continuously.

The CIA triad becomes practical when officers follow secure everyday habits.

Common cyber risks for public institutions

Digital complaint management requires awareness of predictable threats.

Malware

Software designed to damage or control systems.

Insider threat

Risk from careless or malicious internal users.

Social engineering

Manipulating people to reveal information.

Data breach

Unauthorised access or disclosure of records.

Unauthorised access

Weak passwords or stolen credentials.

System failure

Loss of access due to technical disruption.

Risk management requires assessment, awareness, controls, monitoring and audits.

Phishing detection and prevention

Phishing uses deceptive messages to obtain passwords, data or access.

Warning signs

- Suspicious sender address
- Urgent or threatening wording
- Requests for passwords or codes
- Unexpected attachments
- Unknown web links

Safe response

- Verify the sender first
- Do not open suspicious files
- Do not click unknown links
- Report immediately
- Use approved official channels



Ransomware and service continuity

Ransomware can lock complaint records and halt investigations.

Criminals may encrypt files and demand payment for access restoration. Institutional consequences include service disruption, reputational damage and loss of public confidence. Prevention requires system updates, endpoint protection and staff awareness. Frequent backups and tested recovery procedures reduce damage.

Backups are not a luxury; they are an operational continuity requirement.



Secure complaint information management

Identity theft, passwords and MFA

User identity is the first gate protecting digital complaint systems.

Good password practice

- Create strong, unique passwords
- Do not share passwords
- Change compromised passwords quickly
- Use password tools where approved
- Avoid writing passwords openly

Multi-factor authentication

- Adds a second verification step
- Reduces credential misuse
- Protects sensitive systems
- Strengthens identity assurance
- Should be enabled for critical platforms



Safe email practices

Email remains one of the most common channels for cyber attacks.

Use official email accounts for official business.
Verify sender identity before acting on sensitive requests.
Avoid unknown attachments and suspicious links.
Encrypt or protect confidential information where required.
Report suspicious messages promptly through approved channels.

Pause before you click; verify before you share.



Secure complaint information management

Cloud security and digital records protection

Cloud tools are useful only when access, storage and backups are properly controlled.

Access control

Limit access according to official roles.

Secure backup

Maintain retrievable copies of records.

Retention

Follow records lifecycle requirements.

Encryption

Protect data during storage and transfer.

Monitoring

Review logs and suspicious activity.

Compliance

Use cloud services consistent with policy.

Digital records must be protected throughout their lifecycle.

Nigeria Data Protection Act responsibilities

Personal information must be processed lawfully, fairly and responsibly.

Collect and process only information needed for legitimate complaint administration.

Protect complainant records from unauthorised access or disclosure.

Maintain secure storage, access controls and audit trails.

Promote compliance through staff awareness and documented procedures.

Lawful data handling is part of administrative justice.



Secure complaint information management

Confidentiality, privacy and responsible sharing

Information should be shared only when authorised and necessary for official work.

Confidentiality practices

- Restrict access to authorised officers
- Secure confidential documents
- Maintain professional discretion
- Use need-to-know sharing
- Document sensitive disclosures

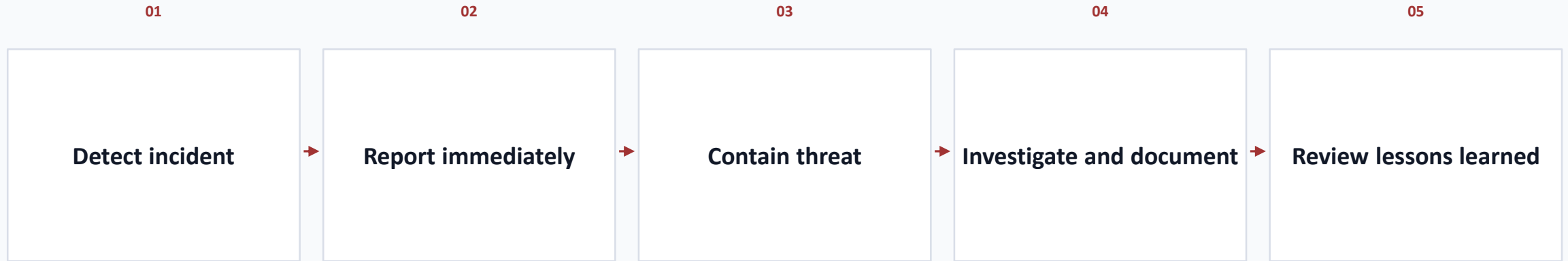
Privacy practices

- Collect only necessary data
- Use personal data for lawful purposes
- Limit unnecessary copying
- Protect files during transfer
- Respect complainant dignity



Incident reporting process

Timely incident reporting limits damage and improves institutional learning.



Do not hide incidents; prompt reporting protects the Commission and the public.



Facilitator prompt: Where does delay occur most often in your current process?

Business continuity and disaster recovery

The Commission must continue essential Ombudsman services during disruptions.

Business continuity

How essential services continue during crisis.

Alternative work

Backup communication and operational arrangements.

Critical records

Protect complaint records before disruption.

Disaster recovery

Restore systems, services and data after incidents.

Recovery objectives

Define acceptable downtime and data loss.

Testing

Review and practise recovery plans regularly.

Prepared institutions recover faster and maintain public confidence.

Module 4 practical exercise

Scenario

An officer receives an urgent email requesting a password reset and a copy of complaint records. The sender name looks official, but the email address is unusual.

Participant tasks

- Identify phishing indicators.
- State immediate response steps.
- Prepare an incident report outline.
- Recommend preventive measures for the office.

Expected output

Cyber incident response checklist

