End-to-End Cybercrime Reporting Process Flow

Step 1: Report Submission

- A **Guest User** or **Registered User** initiates a **report**.
- They access a **form** to provide:
  - Type of cybercrime
  - Incident description
  - Time/date of occurrence
  - Attachments (evidence, screenshots, etc.)
  - Etc …
- User submits the form via:
  - **Anonymous submission** (Guest)
  - **Authenticated submission** (Registered)

Step 2: Input Validation

- System checks:
  - Required fields are filled with an appropriate format
  - No malicious content (e.g., XSS or SQL injection, malicious links …)
  - Valid file types and size
- If input is invalid:
  - The user is notified to correct and resubmit

Step 3: Store and Acknowledge

- Valid report is saved into the **Incident Database**
- A unique **Tracking ID** is generated
- The system sends:
  - A confirmation message
  - A copy of the tracking ID
  - Instructions for follow-up (if needed)

Step 4: Officer Review and Categorization

- An **Officer** retrieves the report
- Officer:
  - Reviews content
  - Classifies the case (e.g., phishing, fraud, ransomware)
  - Sets priority (e.g., urgent, low-risk)

Step 5: Admin/Officer Case Assignment

- The case is assigned to a specific **investigator**
- Status is updated in the **Case History Logs**
- The investigator is notified via the system

Step 6: Request for More Information (Optional)

- If data is missing or unclear:

  - The officer sends a follow-up question
  - User is notified via email or app
  - User responds, and the response is recorded

Step 7: Investigation & Status Updates

- The investigator works on the case
- Periodic updates are:
    - Entered into the system (e.g., “In Progress,” “Under Review”)
    - Visible to the **Registered User** via the **Track Status** feature

Step 8: Case Resolution

- When resolved:
    - Final remarks are logged
    - Case status is marked **"Closed."**
    - Reporter (if registered) is notified (Through **Recommendations)**
    - The case is archived in the **Case History Logs**

About Us

Empowering Communities to Report Cybercrime

The **Cybercrimes Reporting and Awareness System** is a secure, digital platform designed to empower citizens to report cybercrime incidents easily and anonymously. It serves as a bridge between the public and law enforcement agencies, facilitating the timely reporting of cyber-related offenses such as online fraud, identity theft, cyberbullying, and other digital threats.

Working Together with Law Enforcement

This system enables seamless collaboration with authorized law enforcement officers who receive and manage submitted reports. Through a dedicated officer dashboard, authorities can review evidence, track case progress, and communicate updates. By fostering transparency and accountability, the platform strengthens trust and responsiveness in addressing cybercrime.

Our Mission

Our mission is to create a safe and informed digital community by:

- Providing a user-friendly and anonymous platform for citizens to report cybercrimes.
- Equipping officers and administrators with tools for effective case management and response.
- Offering educational resources and awareness materials to help users prevent and recognize cyber threats.
- Supporting data-driven strategies for public safety and cybercrime prevention.

Together, we are building a smarter, safer digital society — where everyone has a voice in the fight against cybercrime.