Reports incidents saves Data

Incidentdb

user

Retrieve data

admin

Sends alerts & notification

Notification&alerts

Manages Users & Reports

**LEVEL 0 DFD**

**Level 0 DFD: Cybercrime Reporting System**

The **Level 0 DFD** represents the high-level view of the **Cybercrime Reporting System** and its main interactions with external entities like **users** and **administrators**. It includes the fundamental processes and data flows within the system.

**Entities and Processes in Level 0 DFD:**

1. **User (External Entity)**
   * Users can **report incidents** related to cybercrime.
   * The system **stores incident data** for further processing.
2. **Admin (External Entity)**
   * The admin can **retrieve data** related to reported incidents.
   * Manages user reports and takes necessary actions.
3. **Notification & Alerts**
   * The system **sends alerts and notifications** to both users and administrators.
   * Helps in scam awareness and real-time updates on incidents.
4. **Incident Database (IncidentDB)**
   * Stores all incident-related information.
   * Maintains records of reported cases and their statuses.

**LEVEL 1 DFD**

Login/register store

User\_db

admin

user

Scam awareness

Creates scam alerts save alerts

Upload Evidence

Incidentdb

Store files

user

incident

Report incident save incident

admin

checks Notify/alert

user

The **Level 1 DFD** provides a more detailed view of the processes inside the system. It expands on the functionalities of **user authentication, incident reporting, scam awareness, and notifications**.

**Entities and Processes in Level 1 DFD:**

1. **User Authentication**
   * Users must **log in or register** before accessing the system.
   * The system verifies credentials and stores user details in **User\_db**.
2. **Scam Awareness Alerts**
   * Admins and the system can create **scam alerts** to warn users about cyber threats.
   * These alerts are stored and managed within the system.
3. **Incident Evidence Management**
   * Users can **upload evidence** related to reported incidents (documents, screenshots, etc.).
   * Evidence is stored in the **IncidentDB** for reference.
4. **Incident Reporting**
   * Users report incidents, and the system **stores files** related to them.
   * Admins can **view and process** reported incidents.
5. **Notification & Alerts**
   * Users **check for updates** on reported cases.
   * The system **notifies users and admins** about incident progress, status changes, or scam alerts.