



MAURITIUS POLICE FORCE




Units involved

- Police Station /CCID
- CID/Cybercrime unit
- Police IT Forensic Lab
- Police Prosecution Office



MAURITIUS POLICE FORCE




Reporting of cybercrime cases

Cases of cybercrime are reported at Police Stations or at the Central CCID.

Police Station	Central CCID
----------------	--------------

Preliminary actions are taken :

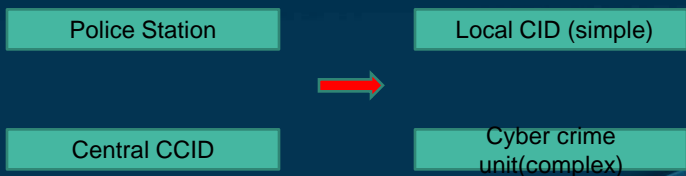
- recording of declaration
- recording of statement



MAURITIUS POLICE FORCE


Reporting of cybercrime cases

Cases are then referred to Cyber crime unit/local CID for investigations.



```

graph LR
    PS[Police Station] --> LCID[Local CID (simple)]
    CCID[Central CCID] --> CCU[Cyber crime unit (complex)]
  
```



MAURITIUS POLICE FORCE


PART III - INVESTIGATIONS AND PROCEDURES of the CMC ACT

Powers of access, search and seizure for the purposes of investigation


(1) Where an investigatory authority has reasonable grounds to believe that stored data would be relevant for the purposes of an investigation or the prosecution of an offence, it may apply to a Judge in Chambers for the issue of a warrant to enter any premises to access, search and seize such data.

(2) In the execution of a warrant under subsection (1), the powers of the investigatory authority shall include the power to –

- seize or secure a computer system or any information and communication technologies medium;
- make and retain a copy of such data or information;
- maintain the integrity of the relevant stored data or information; or
- render inaccessible or remove the stored data or information from the computer system, or any information and communication technologies medium.



MAURITIUS POLICE FORCE




Procedures for handling digital evidence


Search / seizure

- team constituted
 - Enquiry officer (cybercrime/CID)
 - Exhibit officer
 - IT officer
 - Photograph/ Document officer

- Under the authority of an order




MAURITIUS POLICE FORCE




Procedures for handling digital evidence

- **maintain the integrity**
- **maintain the chain of custody**
- **avoid contamination**
- **secure volatile data**
- **proper packing and sealing of exhibit**
- **documentation**



MAURITIUS POLICE FORCE

Examination for digital evidence




```
graph LR; A["Cyber crime unit/CID -  
Investigators / Exhibit  
officer"] --> B["IT Unit -  
Forensic examiners"]
```

The exhibit is sent to the IT Unit forensic lab for examination.

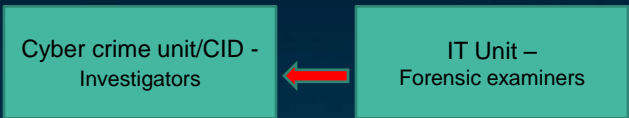
A team of qualified officers carry out forensic examination to search for digital evidence.

The lab is equipped with necessary tools to carry out the examination.



MAURITIUS POLICE FORCE

Examination for digital evidence



```
graph LR; B["IT Unit -  
Forensic examiners"] --> A["Cyber crime unit/CID -  
Investigators"]
```

After examination a technical report is submitted to the investigating officer (Cybercrime unit/CID)

Report include:

- Findings
- IP address
- Email headers
- Phone logs
- Snapshots..

