MOROIL
SINCE 1968

CCTV POLICY

Table of Contents

1. Scope

1.1. This CCTV Policy (hereafter "Policy") applies to **Mauritius Oil Refineries Ltd** (hereafter "**Moroil**").

1.2. **Moroil** has in place a Closed-Circuit Television Systems (hereafter "CCTV system") across its premises. This Policy details the purpose, use and management of the CCTV system at **Moroil** and details the procedures to be followed to ensure that **Moroil** complies with relevant legislation and guidance.

1.3. **Moroil** will have due regard to the Data Protection Act 2017 (hereafter "**DPA**").

1.4. This Policy is also based upon the following documents issued by the Data Protection Office:

- Template on CCTV Policy; and
- Guidelines to regulate the processing of personal data by video surveillance systems (Volume 5).

1.5. This Policy and the procedures therein detailed, apply to all **Moroil**'s CCTV system capturing images of identifiable individuals for the purpose of viewing and/or recording the activities of such individuals in line with Section 4 of this policy. CCTV images are monitored and recorded in strict accordance with this Policy.

2. Roles and Responsibilities of the CCTV System Owner

2.1. The CCTV system is owned by **Moroil**. The CCTV system owner (hereafter the "System Owner") is responsible for the overall management and operation of the CCTV system. Contact details of the System Owner are as follows:

- System Owner: Mauritius Oil Refineries Ltd
- Email address: lpurmessur@moroil.mu
- Address: Quay Road, Port Louis, Mauritius

2.2. **Moroil** remains accountable for lawful processing of personal data in the use of the CCTV system.

2.3. The System Owner has the following responsibilities:

2.3.1. Ensure the conditions of lawful basis are met (see Section 5).

2.3.2. Ensure that the use of CCTV system is implemented in accordance with this policy.

2.3.3. Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes.

2.3.4. Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy.

2.3.5. Ensure that the CCTV monitoring is consistent with the highest standards and protections.

2.3.6. Review camera locations and be responsible for the release of any personal data or recorded CCTV materials stored in compliance with this policy.

2.3.7. Maintain a record of access (e.g., an access log) to or the release of images or any material recorded or stored in the CCTV system.

2.3.8. Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events.

2.3.9. Give consideration to both staff and customer feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.

2.3.10. Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the business and be mindful that no such infringement is likely to take place.

2.3.11. Ensure that adequate signage at appropriate and prominent locations is displayed as detailed in this policy.

2.3.12. Ensure that monitoring images are stored in a secure place where access is restricted to authorised personnel only.

2.3.13. Ensure that images recorded on tapes/DVDs/digital recordings are stored for a maximum period of 60 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Data Protection Officer (hereafter "**DPO**").

2.3.14. Ensure that camera control is solely to monitor suspicious behaviour and criminal damage (amongst others) and not to monitor individual characteristics.

2.3.15. Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.

2.3.16. Ensure that where the Mauritius Police Force requests to set up mobile video equipment for criminal investigations, legal advice has been obtained and such activities have the approval in writing of the **DPO**.

2.3.17. Ensure that staff operating the CCTV system have been adequately trained in the application and use of this policy.

2.3.18. Ensure that **Moroil** conducts a Data Protection Impact Assessment for changes to the CCTV system or for new implementation of a CCTV system.

3. Description of the CCTV System

3.1. System components

- Fixed position cameras
- Pan Tilt and Zoom cameras
- Monitors
- Multiplexers
- Network Video Recording
- Public information signs

3.2. CCTV camera locations

3.2.1. CCTV cameras will be located at the following points on the premises of **Moroil** at different places as provided in Appendix 1.

3.2.2. No camera will be hidden from view.

3.3. Signage/Notification

Signs are prominently placed at the following points on **Moroil**'s premises to inform staff, visitors, customers, and members of the public that a CCTV system is in use for them to choose whether they want to enter a monitored space or not:

- Main Gate 1 & 2
- Warehouse
- Spare Parts building
- Bottling Plant
- Refinery entry
- Reception (Conference Room)

3.4. **Recording**

The CCTV system will provide a 24-hours per day and 7-days per week recording over all locations where a CCTV camera is placed.

3.5. **Effectiveness**

Although every effort has been made to ensure maximum effectiveness of the CCTV system, it is not possible to guarantee that the CCTV system will detect every incident taking place within the area of coverage.

4. Purpose of the CCTV System

4.1. The CCTV system has been installed by **Moroil** for the purposes of reducing the threat of crime generally, identifying disciplinary infringements in **Moroil**'s office compound, assisting in providing evidence where required, protecting **Moroil**'s premises and property as well as helping to ensure the safety of all **Moroil**'s staff, customers, and visitors consistent with respect for the individuals' privacy.

4.2. These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent.
- Assist in the prevention and detection of crime.
- Assist in theft prevention and prosecution.
- Facilitate the identification, apprehension, and prosecution of offenders in relation to crime and public order.
- Facilitate the identification of any activity/event which might warrant disciplinary proceedings being taken against staff and assist in providing evidence to managers and/or to a member of staff against whom disciplinary or other action is threatened to be taken.
- Monitoring of operations.
- Provide management information relating to employee compliance.
- Prevent or respond to bullying in the office compound.
- Prevent or respond to truancy in the office compound.
- Prevent or respond to smoking in non-smoking areas.
- Be aware of any other disciplinary infringements in the office compound.

- Check staff behaviour in the office compound.
- Check visitor behaviour in the office compound.
- Check security in and around the office compound.
- Aid in crime investigation inside the office compound.
- Assure personal safety in the office compound.
- Assist in dispute resolution in the office compound.
- Protect staff from outside threats.
- Check whether physical entry controls are being respected.
- Ensure secure areas are used by authorised personnel only.
- Monitor suspicious transaction

4.3. Five observation categories have been defined based on the relative size that a person appears on screen, of which the business will be able to decide which categories best reflect the type of activity being observed. The observation categories are as follows:

- Monitoring and Control – to oversee a large area or wide field of view;
- Detection – to be alerted to the presence of activity in the field of view;
- Observation – to be able to observe characteristics within a moderately sized field of view;
- Recognition – to be able to identify a known person or object within the field of view; and
- Identification – to be able to clearly identify an unfamiliar individual or object within the field of view.

4.4. CCTV images captured by the CCTV system may be further processed for the conduct of proceedings in any court. This may also require the retention period be increased for this further processing purpose.

4.5. The CCTV system will not be used:

- For hidden or covert recording
- To monitor staff, work performance on a daily basis
- To provide recorded images for the world-wide-web; and
- For any automated decision taking.

5. Legal Basis of Processing

5.1. The use of the CCTV system is in the legitimate interests of **Moroil**, namely:

- For security purposes;
- For verification in case of any accident/incident;
- For operational purposes; and
- For monitoring.

5.2. Only specific (and relevant) individuals/locations should be recorded.

5.3. If no evidence is obtained within a set timeframe, the surveillance should cease. If the surveillance is intended to prevent crime, then covert cameras may be considered to be a more appropriate measure, and less invasive of individual privacy.

6. Retention Period and Back Up of CCTV Images

6.1. CCTV images will be retained for a period adequate to fulfil the purposes specified. This will normally be for a maximum period of 45 to 60 days. After this period, the CCTV images will be automatically overwritten.

6.2. However, any footage that shows an offense or any misconduct will be kept as long as it is needed to undertake criminal proceedings or disciplinary procedures.

7. Security Measures

7.1. The System Owner will ensure compliance with Section 31 of the **DPA**, namely implement all appropriate security and organisational measures to prevent any unauthorised access, alteration, disclosure, accidental loss, and destruction of images captured by the CCTV system.

7.2. In order to protect the CCTV images and footage, **Moroil** will provide the following security measures:

- Having an audit trail to monitor staff access to the footage
- Secure storage of backups
- Secure asset disposal once a hard drive storing **CCTV** images has come to the end of its use

- Allowing only authorised personnel to get access to the **CCTV** room
- Using password protection to manage staff access to stored footage

8. Access to CCTV Images and Footage

All access to **CCTV** images or footage will be recorded in an access log.

8.1. Access to CCTV images and footage by staff

8.1.1. Access to images or footage will be restricted to those staff who need to have access in accordance with the purposes of the CCTV system.

8.1.2. All staff who will be required to deal with the CCTV system will be made aware of the sensitivity of handling images and recordings. CCTV system**.** The **System Owner** will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV.

8.1.3. Training should go to the extent of staff who receive, analyse, and approve requests for CCTV information/images.

8.1.4. Staff access to the system will be limited through appropriate use of secure log-on and access procedures.

8.2. Access to CCTV images and footage by third parties

8.2.1. Access to and the disclosure of CCTV images or footage to third parties should be restricted and carefully controlled to ensure the rights of individuals are protected.

8.2.2. Disclosure should be made in limited and prescribed purposes. The chain of evidence must remain intact if the images or footage are required for evidential purposes. Reasons for the disclosure must be compatible with the purpose for which the images or footage were originally recorded.

8.2.3. Disclosure of recorded material will be limited to the following authorities:

- Law enforcement agencies where the recorded material would assist in a criminal enquiry and/or the prevention of terrorism and disorder;
- Prosecution agencies;
- Relevant legal representatives;
- The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime;

- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings; and
- Emergency services in connection with the investigation of an accident.

8.3. **Access to CCTV images and footage by a data subject**

8.3.1. Images or footage captured by the CCTV system, if they show a recognisable person, are personal data and are covered by the **DPA**.

8.3.2. Any data subject is entitled to ask for a copy of the personal data upon written request, subject to exemptions contained in the **DPA** (section 37 of the **DPA**).

8.3.3. However, they do not have the right of instant access. If there are other identifiable people in the recorded material, **Moroil** will look at options to protect those people's privacy,.

8.3.4. A person whose image has been recorded and retained and who wishes access to the personal data must apply in writing to the **System Owner** (see contact details in Section 2.1).

8.3.5. The **System Owner** will liaise with the Data Protection Officer to ensure that the process mentioned in our Data Subject Rights Request Policy and Procedure is followed. Contact details of the Data Protection Officer can be found in the Privacy Notice published on our website.

8.3.6. It must also be noted that the **System Owner** is reachable to members of the public during office hours. Employees staffing the contact point should be aware of the appropriate policies and procedures.

8.3.7. For any other data subject requests, the **System Owner** will ensure that **Moroil** will comply with the requirements of the **DPA** through an annual review of the CCTV system with the Data Protection Officer.

9. Complaints Procedure

9.1. It is recognised that members of **Moroil** and members of the public may have concerns or complaints about the operation of the CCTV system.

9.2. Any complaint should be addressed in the first instance to the System Owner who will liaise with the Data Protection Officer.

9.3. The System Owner will be available during the office hours from Monday to Friday except when **Moroil** is officially closed.

9.4. The CCTV Policy should be provided as a source of further information, either at the information desk, reception or cashier or displayed on an easily accessible poster or website.

9.5. Upon request, enquirers will be provided with a Subject Access Request Form if required or requested, to exercise any right a data subject has.

10. Monitoring Compliance of the CCTV System

10.1. The Data Protection Officer is responsible for ensuring day to day compliance with the **DPA**.

10.2. All CCTV recordings will be handled in strict accordance with this policy.

10.3. The effectiveness of the CCTV system and all documented procedures will be kept under review and a report from the Data Protection Officer will be periodically made to the Managing Director in **Moroil**. This will happen at least once per calendar year.

DocuSigned by:
Clarenc Jerome Paul Edouard
2650E28BDB5C4FC...
Date: 14 February 2025

Approved by: Clarenc Jerome Paul Edouard

Managing Director

APPENDIX 1

Camera	Department Concerned	Camera Range
1	General	Gate 5
2	General	Loading Bay 1 / Tuna
3	General	Motorcycle Parking / Main Road
4	General	Oil Complex Entrance / Gate 4
5	General	Oil Complex Gate 3
6	General	Oil Complex Parking
7	General	Yard / Main Gate 2 / Filling
8	Human Resource	Gate 2 / Next to Lorry Parking
9	Human Resource	Main Parking & Loading Bay 2
10	Human Resource	Main Parking (1)
11	Human Resource	Moroil Main Entrance
12	Human Resource	Reception
13	Human Resource	Security Gate Post 1
14	Human Resource	Security Gate Post 2
15	Human Resource	Staff Mess Room Entrance
16	Human Resource	Workers Canteen
17	IT	Server Room Corridor
18	Logisitics	Filling Station
19	Logisitics	Sales Yard
20	Packaging	Bottle Manufacturing
21	Packaging	Bottling Exit
22	Packaging	Bottling Line 1
23	Packaging	Bottling Line 2
24	Packaging	Bottling Line 3
25	Packaging	Drum Plant
26	Packaging	Drum Plant / Filling Machine
27	Packaging	Ex Conference / New Packaing
28	Packaging	Ex Conference / New Packaing 1
29	Packaging	Ex Pouch / Main Entrance
30	Packaging	Gallon Filling
31	Packaging	New Bottling Machine 1
32	Packaging	New Bottling Machine 2
33	Packaging	New Bottling Machine 3
34	Packaging	New Bottling Machine 4
35	Packaging	New Bottling Machine 5
36	Packaging	New Bottling Machine 6
37	Packaging	New Generator
38	Packaging	Packaging Entrance
39	Process	Acid Oil Plant / Corridor
40	Process	Boiler Entrance
41	Process	Laboratory Corridor
42	Process	Loading Bay 1

43	Process	Oil Complex
44	Process	Oil Complex / Tank Farm Corridpr
45	Process	Refinery First Floor
46	Process	Refinery Ground Floor 1
47	Process	Refinery Ground Floor 2
48	Process	Refinery Ground Floor 3
49	Process	Refinery Second Floor
50	Process	Refinery Tank Farm 1
51	Process	Refinery Tank Farm 2
52	Process	Tank Farm Back / PIM Corridor
53	Process	Wetland
54	Process	Wetland 2
55	Sales & Marketing	Moroil Boutique
56	Sales & Marketing	Retail Shop Coridor
57	Sales & Marketing	Sales Back Door
58	Sales & Marketing	Sales Corridor
59	Sales & Marketing	Sales Main Entrance
60	Sales & Marketing	Sales Main Exit Door
61	Warehouse	Main Store 1
62	Warehouse	Main Store 2
63	Warehouse	Main Store 3
64	Warehouse	Main Store 4
65	Warehouse	Main Store Entrance
66	Warehouse	New Store 1
67	Warehouse	New Store 2
68	Warehouse	New Store 3
69	Warehouse	New Warehouse 1
70	Warehouse	New Warehouse 2
71	Warehouse	New Warehouse 3
72	Warehouse	SAS 1
73	Warehouse	SAS 2
74	Warehouse	SAS 3
75	Warehouse	SAS Entry 1
76	Warehouse	Store 3
77	Warehouse	Store 3 Main Entrance
78	Warehouse	Store Spare Part
79	Warehouse	Store Spare Part 1

Date: 17.01.2025