



## **CCTV POLICY 1.0**

### **1. PURPOSES**

**1.1.** The Office of the Ombudsperson for Financial Services (the "Office") has in place a CCTV system, managed and controlled by the Office.

**1.2.** The principal purposes of the Office CCTV system, amongst others, are as follows:

- To ensure the security of its premises, records, assets and equipment.
- To ensure the safety of all Office employees, complainants, suppliers, visitors, and other stakeholders.
- To assist in the investigation of law enforcement agencies or the Office of any illegal or suspected activities committed at the Office by any person.
- To assist in the investigation of disciplinary infringements or malpractices in the Office compound.

### **2. SCOPE**

**2.1.** CCTV Cameras are found at the following locations in the Office:

- Main Entrances/Exits
- Reception & Visitors' Area
- Entrances and Exits of Staff Office Areas
- Corridors
- Store and Filing Areas
- Server Room

**2.2.** The CCTV system provides a 24-hours per day and 7-days per week continuous recording over all the locations where a CCTV camera is placed.

**2.3.** There will not be constant or unnecessary viewing of the images or focus on Staff or specific individuals. The privacy of all individuals will be safeguarded, and the use of the CCTV system, will be in accordance with the Data Protection Act 2017.

### **3. SIGNAGE/NOTIFICATION**

A signage is posted at the main entrance of the Office.

### **4. RETENTION PERIOD AND BACKUP**

- 4.1. CCTV images will not be retained for longer periods than necessary and will be retained for a period adequate to fulfil the purposes specified. This will normally be for a minimum period of 6 months.
- 4.2. After the retention period, the Secretary shall ensure that recordings are deleted.
- 4.3. Any footage that shows an offence or any misconduct will be kept as long as it is needed to undertake criminal proceedings or disciplinary procedures.
- 4.4. All retained CCTV footages shall be stored securely, and correct backup shall be done periodically and kept safely under lock and key on site.

### **5. SECURITY MEASURES**

5.1. The Office will ensure compliance with Section 31 of the Data Protection Act 2017, namely implement all appropriate security and organisational measures to prevent any unauthorised access, alteration, disclosure, accidental loss, and destruction of CCTV footages.

5.2. In order to protect the CCTV images and footages, the Office provides the following security measures:

- Using a Network Video Recorder (NVR) to store footage in a secured location on site
- Backing up of the footages securely on site

- Allowing only authorised personnel to access the CCTV images/room
- Keeping a logbook to monitor access to footages
- Using password protection to manage access to stored footage
- Transmitting and storing of stored footage in encrypted form
- Doing regular audits of system security.

## **6. DISCLOSURE OF CCTV FOOTAGE**

Disclosure of recorded materials, subject to its availability, will be limited to the following:

- Law enforcement agencies where the recorded material would assist in a criminal enquiry and/or the prevention of terrorism and disorder, including the Police.
- Prosecution agencies.
- Any authorised person or agency to whom disclosure is required by any applicable law, regulation or court order, and will be made subject to strict obligations imposed on these third parties to maintain the confidentiality and integrity of CCTV images as well as safeguarding its security.

## **7. REQUEST FOR ACCESS OF CCTV FOOTAGE**

7.1. Request for the access to CCTV footage will be made in compliance with the Data protection Act 2017, subject to the protection of other persons'/employees' privacy, on receipt of a duly signed letter addressed to the Secretary of the Office.

7.2. However, the person requesting for access does not have the right of instant access. If there are other identifiable person/s in the recorded material, the Office will look at options to protect their privacy.

## **8. PROCEDURES TO HANDLE INCIDENTS**

8.1. It is recognised that members of the Office and of the public may have concerns or complaints about the operation of the CCTV system.

8.2. The Office will operate and manage its CCTV system in accordance with this Policy and the Data Protection Act 2017.

8.2. Any complaint should be addressed, in the first instance to the Secretary of the Office, in writing, who will liaise with the Data Protection Office.

8.3. The procedures for handling of incidents will be in accordance with internal procedures of the prosecution or law enforcement agencies or as alternatively provided by any law or regulation.

8.4. Any breach will entail appropriate action as provided by the Data Protection Act 2017, or disciplinary procedures, or referred to the appropriate law enforcement/prosecution agency.

## **9. Policy Review**

9.1. The Office has the discretion to update this Policy as and when required and thereafter the revised version will be effective.

9.2. It is the responsibility of any person to view this policy periodically and be kept abreast of any modification.

Office of Ombudsperson for Financial Services