



## **CCTV Policy**

**Effective from: 27<sup>th</sup> May 2025**

**Next Review: May 2026**

## **Closed-Circuit Television CCTV Policy**

### **Purpose**

The purpose of this policy is to regulate the use of the Closed-Circuit Television (CCTV) and its associated technology in the monitoring of the internal and external environments of the Organisation's premises. CCTV system is to enhance the health and safety and security of the staff, visitors and property, monitor for theft prevention or damage to the company property, protect against crime, monitor and investigate incidents occurring within the premises, and support disciplinary or legal proceedings, where necessary.

### **Scope**

This policy applies to all MSS employees, contractors, vendors, visitors accessing MSS premises, facilities and resources.

### **Data Controller**

Access to CCTV footage is strictly limited and may only be viewed or released with authorisation from Darren Kiely, and he is the **only** person with direct access to the recorded images.

### **Policy**

#### **1.0. Location of the cameras**

MSS operates a number of cameras which are located in all warehouse areas in Ballymount, Robinhood, Walkinstown and Hibernian. These operate on a 24-hour basis, seven days a week. Cameras are not installed in private areas such as toilets, changing rooms, or staff rest areas.

#### **2.0. Recording and storage**

Recorded images are retained and stored for 30 days from the date of recording.

However, MSS reserves the right to retain images for a longer period where there are required for investigation or legal purposes. After the retention period, footage is deleted or securely overwritten.

Those employees with responsibility for processing CCTV images must only do so in line with established procedures and must ensure the security of the data at all times.

**Any employee who uses the CCTV system or CCTV images in an unauthorised manner may be subject to disciplinary action up to and including dismissal.**

### **3.0. Access and Disclosure**

Unauthorised use is any processing incompatible with the data's original purpose including but not limited to:

- Disclosure of images containing personal data to an unauthorised third party, including other employees;
- Unauthorised processing of personal data in the form of copying the images on to a USB, website or print format;
- Circulation of images containing personal data by email or posing of images containing personal data on the internet.

### **4.0. Rights for individuals**

Under GDPR legislation, individuals have the following rights:

- Right to access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to object

Access to and disclosure of images recorded by the CCTV system is carefully monitored. Access to images by third parties will only be allowed in limited and prescribed circumstances permitted by legislation. Such circumstances may include the disclosure of personal information in order to:

- Safeguard the security of the State
- Prevent, and investigate offences, or collect any tax or monies owed to the State
- Protect the international relations of the State
- Prevent injury or damage to the property
- Meet legal requirements
- Obtain legal advice, for the purpose of legal proceedings
- Meet a request from, or with the consent of, the data subject, or a person acting on his or her behalf.

Request to access imaging contain their personal data needs to be done in writing to Darren Kiely ([darren@mssltd.ie](mailto:darren@mssltd.ie)) and will be responded to within one month, in accordance with GDPR guidelines.

Individuals requesting access to images must supply MSS with the following:

- Adequate information for the images to be located
- Sufficient information to enable MSS to verify that the applicant has a legitimate right to request access
- Proof of identification through photographic identification, for example passport or driving license

In the event that a request for access is denied, the organisation will document the following:

- The identity of the individual making the request
- The date of the request
- The reason for refusing to supply the images requested

The document will then be signed and dated and will be provided to the individual making the data access request.

## **5.0 Term of Validity**

This CCTV Policy becomes effective on 27<sup>th</sup> of May 2025.