CCTV System Policy

**1 Introduction**

1.1 The purpose of the CCTV System Policy of COMPANY is to regulate the management, operation and use of the closed circuit television (CCTV) system (“the System”).

1.2 The system comprises several fixed and dome cameras located around the company site. The Policy follows the Data Protection Commissioner’s published guidelines and is in accordance with Data Protection Legislation.

1.3 The System is wholly owned by the Company.

**2 Objectives of the System**

(a) To act as a deterrent against criminal activity affecting property belonging to the company.

(b) To increase safety of staff, customers and visitors.

(c) The System will not be used to monitor the movements of staff, customers or visitors.

**3 Statement of intent**

3.1 The Company will treat the System and all information, documents and data images obtained and used there from as data which may be deemed personal data requiring protection under the Acts.

3.2 It is intended that the CCTV cameras will be used to capture images of intruders or individuals damaging property or removing goods without authorization, and release this information to and at the request of, the Gardai.

3.3 Information captured as a result of the use of the System will not be used for any commercial purpose. The recorded images shall be stored on DVDs which will only be released to third parties for use in the investigation of a specific crime and with the written authority of the Garda Siochana. DVDs containing personal data will never be released to the media or other third parties for any purpose that is not permitted under the Policy without the Data Subject’s consent.

3.4 The planning and operation of the System has been designed to ensure that it provides maximum effectiveness and efficiency insofar as is reasonably practicable, but it is not possible to guarantee that the System will cover or detect every single incident taking place in the areas of coverage.

3.5 Warning signs, as required by the Code of Practice of the Data Protection Commissioner have been placed at all access points to areas covered by the company CCTVs to inform all persons who may be deemed Data Subjects, of the existence of the System.

**4 Operation of the system**

4.1 For the purposes of Data Protection Legislation the Data Controller will be TITLE. In practice, the System will be managed by the TITLE, in accordance with the principles and objectives expressed in the Policy.

4.2 The day-to-day management of the system will be the responsibility of the Data Controller and be approved by the CEO / MD / GM. Other personnel may also be authorised by the CEO / MD / GM to view recorded images for the purposes outlined in this policy.

4.3 The Data Controller’s office (referred to in 6 below) will only be staffed by the Company’s authorised personnel who shall also adhere to the Policy.

4.4 The System will be operated 24 hours each day, every day of the year, except for periods of breakdown or necessary maintenance.

**5 Control Room**

5.1 The Data Controller’s office is where the system is installed and from where it is controlled. The Data Controller will check and confirm the efficiency of the System regularly and that the equipment is properly recording and that cameras are functional. The recording equipment is to be secured in a locked cabinet in the Data Controller’s office. The key will be held by the Data Controller.

5.2 Access to the Data Controller’s office will be limited to authorised personnel while recorded data is being viewed.

5.3 If out of hours emergency maintenance arises, the Management and or Data Controller must be satisfied of the identity and purpose of contractors before allowing access to the Control cabinet.

5.4 During the working day when the Data Controller’s office is not manned the Control cabinet will be kept locked.

**6 Recording procedures**

6.1 CCTV recording will be maintained at all times.

6.2 CCTV Monitors are installed in the following areas and will be used in accordance with this policy:

(a) Data Controller’s office ***and/or***

(b) A Restricted location. Should this be a remote monitor its use will be restricted to ensure that staff and customer movements are not being monitored or captured continuously.

**7 Video recording procedures**

7.1 Recordings are initially made to a hard disk which is in the locked Control cabinet in the Data Controller’s office. The equipment is programmed to delete images after X days automatically. Data can be recorded on to DVDs for specific purposes in accordance with this policy and with the authorization of the Chief Executive. Such DVDs will be stored in the locked Control cabinet.

7.2 In order to maintain and preserve the integrity of the DVDs used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

(a) Each DVD/Softcopy must be identified by a unique mark.

(b) Before use each DVD/Softcopy must be cleaned of any previous recording.

(c) The Data Controller shall register the date and time of DVD/Softcopy insert, including DVD/Softcopy reference.

(d) A DVD/Softcopy required for evidential purposes must be sealed, witnessed, signed by the Data Controller, dated and stored in a separate and secure, safety container. If a DVD/Softcopy is not copied for the Gardai before it is sealed, a copy may be made later providing that it is then resealed, witnessed, signed by the Data Controller, dated and returned to the evidence DVD store.

(e) If the DVD is archived the reference must be noted.

7.3 DVD/Softcopy may be viewed by the Gardai when requested to assist them in their duties.

7.4 A record will be maintained of the release or viewing of DVDs to the Gardai or other authorised persons. A register will be maintained for this purpose.

7.5 Should a DVD/Soft Copy be required as evidence, a copy may be released to the Gardai under the procedures described in paragraph 7.2 (d) of the Policy. DVDs/Soft copies will only be released to the Gardai on the clear understanding that the recording remains the property of the Company, and both the DVD / Soft copy and information contained on it are to be treated in accordance with this code. The Company also retains the right to refuse permission for the Gardai to pass to any other person the DVD / Soft copy or any part of the information contained thereon. On occasions when a Court requires the release of an original DVD / Soft copy this will be produced from the secure evidence store, complete in its sealed bag.

7.6 The Gardai may require the company to retain the stored copies for possible use as evidence in the future. Such copies will be properly indexed and properly and securely stored until they are needed by the Gardai.

7.7 In respect of copies not required to be retained for security, crime detection or other legitimate purposes, the Company will ensure its best endeavours are used to safely and properly dispose of the contents of the copies after 28 days.

7.8 Applications received from outside bodies (e.g. solicitors) to view or release personal data held by the Company will be referred to the CEO / MD / GM. In these circumstances a copy will be made available for viewing or released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee can be charged in such circumstances: €6.35 for subject access requests; a sum not exceeding the cost of materials in other cases.

**8 Breaches of the Policy (including breaches of security)**

8.1 Any breach of the Policy by the Company staff or any other person with responsibility under the Policy will be initially investigated by the CEO / MD / GM, in order for him/her to take the appropriate disciplinary action.

8.2 Any serious breach of the Policy will be immediately investigated and an independent investigation will be carried out by nominees of the CEO / MD / GM to make recommendations on how to remedy the breach.

**9 Assessment of the System**

9.1 Maintenance and performance of the system, including random operating checks, will routinely be carried out by the Data Controller.

**10 Complaints**

10.1 Any complaints about the Company’s CCTV system should be addressed to the CEO / MD / GM.

10.2 Complaints will be investigated in accordance with paragraphs 8.1 and 8.2 of the Policy.

10.3 Any person who might be deemed a Data Subject in relation to the System shall be at liberty to make a complaint directly to the office of the Data Protection Commissioner.

**11 Access by the Data Subject**

11.1 Data Protection Legislation provide Data Subjects (individuals to whom "personal data" relate) with a right of access to personal data held about themselves (including images recorded by the System and stored on DVD/softcopy), under the terms of the Acts.

11.2 Requests by Data Subjects for such access should be made in writing to the CEO / MD / GM.

11.3 The form of access granted may consist of facilities being offered at the Company premises to view the relevant personal data or the release of a copy of the relevant personal data.

**12 Public information**

Copies of the Policy will be available to the public from the Company Office and the CEO / MD / GM.

Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 CEO / MD / GM

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_