Closed Circuit Television (CCTV) Policy

Video recording through a Closed-Circuit Television (CCTV) system is considered a form of personal data processing and is therefore regulated under applicable data protection legislation, including the General Data Protection Regulation (EU) 2016/679 (GDPR) and Law 125(I)/2018.

We reserve the right to change this policy at any time, and any such changes will be notified to staff, visitors and customers as reasonably possible.

The Company is committed to ensuring that the operation of its CCTV system fully complies with applicable legislation, particularly regarding the principles of transparency, necessity, proportionality, and data security.

Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred to the Data Protection Officer (DPO) at dpo@trustcyprusinsurance.com.

Compliance with the Policy

All staff must comply with this policy and any document referenced in it. We take compliance with this policy very seriously. Failure to comply with the policy puts at risk the individuals whose personal information is being processed, carries the risk of sanctions for the individual and for the Company.

The processing is based on the Company's legitimate interests (Art. 6(1)(f) GDPR), specifically the protection of its premises, personnel, and property.

The Company uses CCTV to provide a safe and secure environment for staff, visitors and customers, and to protect company property. Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action. Non-employees, such as contract staff may have their contract terminated with immediate effect.

Monitored Areas

The Company has installed a CCTV system at its Headquarters in Nicosia and its Regional Offices in Limassol, Larnaca, Paralimni and Paphos. The monitored areas include the main building entrances and exits, common areas such as internal corridors, the server room and areas surrounding the building.

The common areas covered by the CCTV system include the entrance area on each floor between the elevator and the main door, the staircase area, the lobby of each floor, the

courtyard surrounding the building, the kitchen/dining area which has a separate entrance.

To ensure transparency, clearly visible signage has been installed at all monitored areas to inform individuals of the CCTV surveillance in operation, in accordance with legal requirements. Furthermore, a Data Protection Impact Assessment (DPIA) has been conducted to assess and mitigate any potential risks to the rights and freedoms of individuals.

Purposes of the CCTV

The primary purposes of the CCTV system are:

- To maintain a high level of safety for employees and visitors;
- To protect the life and physical integrity of individuals within the premises;
- To detect and prevent unauthorized activities or potential criminal offenses;
- To protect company property and other assets;
- To monitor security and health and safety at our premises;
- To deter crime and assist in the prevention and detection of crime and/or serious breaches of policies and procedures;
- To assist with the identification, apprehension and prosecution of offenders;
- To collect and preserve evidence in the event of an incident involving security concerns;
- To protect the Company's legitimate interests.

We have carried out a data protection impact assessment and consider that these purposes are legitimate, reasonable, appropriate and proportionate.

We have:

- assessed and documented the appropriateness of and reasons for using CCTV;
- established and documented who is responsible for day-to-day compliance with this policy; and
- ensured signage is displayed to inform individuals that CCTV is in operation, and that CCTV operations are covered in appropriate policies.

We keep a record of the CCTV installed and used.

Operation of the CCTV

The CCTV system provides continuous video surveillance *without audio*, and recordings are retained for a period of 28 days (Head Offices) and 12 days (Regional Offices) unless an incident occurs which requires a longer retention period. These periods have been assessed as sufficient to investigate and respond to incidents or complaints, without storing data longer than necessary.

The CCTV system operates 24 hours a day, both during and outside the company's working hours, including night-time, in order to prevent or record incidents such as theft,

vandalism, or other unlawful activities. Special attention is given to the protection of areas where cash amounts are stored, as well as physical files or documents containing sensitive or other personal data of clients and associates. Although these areas are secured and locked, the presence of the CCTV system serves as an additional deterrent, significantly reducing the likelihood of a breach.

The kitchen area at the Company's Head Offices is covered by the CCTV system, which is configured so that no recording takes place during the official hours of use by the staff. Specifically, recording is disabled from 11:00 a.m. to 3:00 p.m. to ensure the privacy of employees during their breaks, which take place between 12:30 p.m. and 2:00 p.m.

Access And Disclosure of CCTV Data

Access to and disclosure of images recorded on CCTV will be restricted and carefully controlled. This will ensure that the rights of individuals are protected, and also that the images can be used as evidence if required. Images may only be disclosed in accordance with the purposes for which they were originally collected.

Access requests by data subjects will be handled in line with the Data Subject Access Request Procedure and the specific principles set out below.

The CEO and the DPO are the only persons who can authorise disclosure of CCTV information. All requests for disclosure should be documented for audit purposes in the CCTV register. If disclosure is denied, the reason should also be recorded. Where a request to retain information is authorised, reasonable steps will be taken to safeguard any footage which may otherwise be deleted.

Access to the CCTV recordings is strictly limited to the IT Manager and the CEO, who are jointly responsible for the secure handling and management of the recorded data. Appropriate technical measures are in place, including user identification controls, to ensure that only authorised personnel can access the recordings and that all access is properly monitored and logged.

Access to and disclosure of images to third parties

Disclosures to third parties will only be made in accordance with the purpose(s) for which the system is used and will be limited to:

a. police and other law enforcement agencies, where the images recorded could assist in a specific criminal enquiry and/or the prevention of terrorism and disorder;
b. relevant legal representatives of people whose images have been recorded and retained;
c. individuals who have been caught on our CCTV in accordance with a request made;

Staff images will only be accessed if a serious event occurs, such as criminal activity, fraud, gross misconduct, or behaviour that puts others at risk.

Access Requests by Employees

In accordance with the rights provided under the GDPR, and to the extent applicable to CCTV surveillance, Employees may request:

- Access to CCTV footage in which they appear, provided their identity can be verified and third-party rights are not infringed;
- Erasure of their personal data captured by CCTV, under certain circumstances;
- Restriction of processing, under certain circumstances;
- Objection to the processing of their personal data, under certain circumstances;

Access to personal data captured by the CCTV footage is only permitted upon written request by an Employee to the DPO, provided the request concerns footage that exclusively depicts the requesting individual. Requests should include the date, approximate time, and location to help identify relevant footage.

Requests by data subjects for access to CCTV images/footage must be made in writing and must include:

- the full name and address of the person making the request (the 'data subject');
- a description of the data subject;
- the approximate date and time when the images were recorded to allow for searching;
- the location where the images were recorded.

All requests will be evaluated to ensure that the rights and freedoms of third parties appearing in the same footage are not infringed. The DPO is obliged to respond to data subjects' requests without undue delay, and within one month at the latest.

The following information must be kept on a CCTV register that will be maintained for that purpose and held by the DPO when media are removed for viewing:

a. the date and time they were removed;
b. the name of the person removing the media;
c. the name(s) of the person(s) viewing the images including the department to which the person viewing the images belongs or, if they are from an outside organisation, the organisation's name (e.g. the police);
d. the reason for viewing the images; and
e. the date and time the media were returned to the system or secure storage (if applicable).

The CCTV system may also capture personal data of visitors and third parties entering monitored areas. The same principles of lawfulness, transparency, and protection apply to all individuals captured.

For any questions or concerns regarding the operation of the CCTV system or the processing of related personal data, Employees are encouraged to contact the Company's Data Protection Officer (DPO) at: dpo@trustcyprusinsurance.com.

Complaints and enquiries about the operation of our CCTV systems should be made directly with the Company's DPO. If a complainant or enquirer is not satisfied with the response received, they can write to the Data Protection Commissioner of the Republic of Cyprus at:

Postal address:
P.O. Box 23378, 1682 Nicosia, Cyprus

Tel: +357 22818456
Fax: +357 22304565

Email: commissioner@dataprotection.gov.cy

Enforcement and Compliance

All authorised users of our surveillance technology and its underlying data are required to adhere to the controls around the use of CCTV as set out in this policy and as may be advised separately from time to time. The use of the CCTV system for any purpose other than those specifically authorised will be subject to a full investigation and could lead to disciplinary action.

The misuse of our surveillance systems and unauthorised use of images and CCTV footage may constitute a criminal offence.

Any concerns regarding the use of CCTV should be shared with your line manager.