COMPLIANCE PROGRAM – GENERAL PERSONAL DATA PROTECTION LAW (LGPD)

VIDEO SURVEILLANCE AND CCTV USE POLICY

Ver. 1.0/2025.

1. INTRODUCTION

Closed-Circuit Television (CCTV) technology has evolved in recent years to become more reliable, cost-effective, and available. When used appropriately, CCTV can help reduce the risk of unauthorized access to facilities, reassure users, and provide an accurate record of events during an incident.

To protect its users, employees, and other stakeholders, FLASH ENGENHARIA utilizes CCTV in appropriate circumstances to address specific risk areas. In collecting and using recorded video data, FLASH ENGENHARIA is subject to various laws, including Law 13.709/18 – General Personal Data Protection Law (LGPD), which governs how such activities must be conducted and the safeguards required to protect recorded video data.

The objective of this policy is to define the rules to be followed to ensure that FLASH ENGENHARIA's responsibilities are met at all times and that the utility of recorded data complies with legal determinations.

2. OBJECTIVE

2.1 The equipment used in the CCTV system is intended for the safety of employees, users, suppliers, and visitors, as well as the protection of assets and information, aiming to prevent theft, sexual harassment, and internal security risks. The use of this equipment for deterrence may result in investigations and potential criminal proceedings for suspicious and/or criminal behavior.

2.2 FLASH ENGENHARIA (CNPJ No. 04.844.206/0001-59), headquartered at Rua Professora Celia Cangro Marques Mendes, No. 1000 - Alto da Boa Vista – Sorocaba, SP, operates a video surveillance protection system throughout its facilities for the strict purpose of promoting corporate safety and protection. This complies with Law 13.709 (LGPD), Ordinance No. 3.233/2012/DG/DPF (Private Security Instructions), Art. 5 of the 1988 Constitution of the Federative Republic of Brazil, and the CLT (Consolidation of Labor Laws), following guidelines from the ANPD (National Data Protection Authority).

2.3 This policy does not cover specialized technology such as Automatic Number Plate Recognition (ANPR), facial recognition, or remotely operated vehicles (drones/UAS).

2.4 This policy applies to all operations, personnel, and processes of FLASH ENGENHARIA’s information security systems, including board members, directors, employees, and third parties who may have legitimate access to the CCTV system.

3. DATA PROTECTION

3.1 The system serves a specific and legitimate purpose to address risks, such as crime prevention in areas subject to illegal activities.

3.2 Following the Data Minimization principle (LGPD), video recording shall be active only when necessary. Audio recording will only be used when justified, considering privacy concerns. FLASH ENGENHARIA acts as the Data Controller.

3.3 Third parties involved in processing (storage/maintenance) are considered Processors under the LGPD, requiring a valid service agreement.

3.4 A Data Protection Impact Assessment (DPIA) must be performed for each new device implementation and reviewed regularly. The legal basis for processing is the promotion of corporate safety and security.

3.5 An annual review of this policy's compliance with data protection rules will be conducted.

4. COVERED AREAS

4.1 Camera placement focuses on maintaining a security perimeter and controlling external access. Coverage includes internal and external spaces under FLASH ENGENHARIA's responsibility. To respect privacy (Art. 5, X), cameras are not specifically focused on individual employees.

4.2 Cameras are located at strategic points, including production warehouses, external perimeters, and gatehouses. Locations are carefully analyzed to ensure surveillance is limited to relevant spaces.

5. SIGNAGE

5.1 Areas monitored by video surveillance must be signaled with signs or notices. The text must comply with the Transparency Principle defined in the LGPD.

6. STORAGE AND RETENTION

6.1 Standard image retention is between 7 and 45 days, or the maximum capacity supported by the recording hardware.

6.2 Storage must be in a secure location with access restricted to authorized personnel.

6.3 Records categorized as "surveillance logs" shall be retained in secure local storage for no more than 02 (two) years, after which they must be deleted or overwritten, unless part of a criminal investigation or legal proceeding.

6.4 Editing, altering, or intercepting recordings is strictly prohibited, except to improve quality for investigations or to blur features.

6.5 Blurring the faces of non-participants in an incident is the only authorized modification for privacy reasons when providing images to third parties.

6.6 Monitors must be configured to prevent unauthorized duplication or tampering.

6.7 All storage and access are controlled by the Occupational Safety Department.

6.8 Recordings used in law enforcement investigations must be retained until the end of the legal process and appeal period. Transmission over the internet must use encryption.

7. ACCESS MANAGEMENT AND MONITORING

7.1 Access to live or recorded video is limited to the security sector and designated personnel. Copying or retransmission must be pre-authorized by the IT DEPARTMENT Manager. Employees are prohibited from disclosing information acquired from

cameras for non-official purposes.

7.2 Data deletion must be approved by the IT DEPARTMENT following the DPO's (Data Protection Officer) guidelines.

7.3 The IT DEPARTMENT shall maintain a log of all instances of access, including the date and identity of the person granted access.

7.4 Access logs must be maintained for a minimum of 12 (twelve) months.

7.5 Access requests by Data Subjects must be justified by a specific interest and supported by LGPD legal bases.

7.6 Internal requests for video access must be submitted in writing to the IT DEPARTMENT for analysis and approval by the DPO.

7.7 External requests for video data release must be formally submitted to the LEGAL DEPARTMENT and the DPO for approval.

7.8 Legal demands (subpoenas, warrants) must be forwarded to the LEGAL DEPARTMENT, which is responsible for reviewing and responding to law enforcement.

7.9 Data subjects may exercise their rights (access, correction, deletion) regarding CCTV data via email: lgpd@flashengenharia.com.br.

8. LAST UPDATE AND PREVIOUS VERSIONS

Last updated: December 16, 2025.