**CCTV/Surveillance Policy**

# 1. Policy Purpose

This policy outlines the use of CCTV surveillance by IntellOperations Ltd (“IntellOperations”, “we”, “our”, “us”) to support business owners in protecting their assets, ensuring public safety, and maintaining a healthy and secure community environment.

We work closely with law enforcement agencies to ensure that anti-social behaviour and criminal activity are properly reported and investigated. As a community-focused team, we monitor the public within retail and storefront environments to protect property, deter unlawful behaviour, and submit evidence of public incidents directly to the police.

# 2. Scope

This policy applies to all remote surveillance services provided by IntellOperations Ltd. CCTV systems are owned and installed by the client (store owners), and we only monitor footage that has been explicitly approved and shared with us.

- We do not install or operate additional surveillance equipment.
- We monitor only the agreed-upon CCTV feeds as authorised by the client.

# 3. Legal Basis for CCTV Use

Our CCTV monitoring practices are conducted in accordance with the following legal bases:
- Legitimate Interests: Surveillance is conducted to prevent and respond to criminal behaviour. All offences observed are reported to the police.
- Legal Obligation: CCTV evidence is collected, securely stored, and linked to specific case files before being reported to law enforcement. Each incident is submitted with a corresponding Crime Reference Number.
- Consent: While client stores are privately owned, they are open to the public. With signed consent from the store owner, we are authorised to monitor their CCTV systems.

Relevant legislation includes:
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Surveillance Camera Code of Practice

This policy applies to store clients, employees, store visitors, and any individuals captured on camera within monitored premises.

# 4. System Overview

CCTV systems monitored by IntellOperations may include:
- Fixed-position cameras
- PTZ (pan-tilt-zoom) cameras
- Remote-access video feeds

Cameras may be:
- Audio-enabled (if configured by the client)
- Motion-activated or continuously recording
- Monitored live during operating hours (not 24/7)
- Integrated with basic motion detection (no facial recognition is used)

# 5. Monitoring and Access

- All footage is monitored by trained and authorised staff at IntellOperations.
- Access to surveillance feeds is controlled and requires approval from the Monitoring Department’s Team Manager.
- Monitoring is conducted during scheduled operational hours (not 24/7).
- All access is logged and subject to internal audit procedures.

# 6. Data Storage & Retention

- CCTV footage is retained for a maximum of 30 days unless flagged as part of an ongoing investigation or legal requirement.
- Data is securely stored in encrypted cloud storage systems managed in compliance with data protection standards.
- Upon reaching the 30-day threshold, footage is securely deleted. IntellOperations collaborates with the client store to ensure deletion is confirmed and completed.

# 7. Access to Footage

Only the following roles are authorised to access surveillance footage:
- Operations Managers
- Team Managers
- Designated and signed-off IntellOperations staff

Footage may only be shared with external parties under the following conditions:
- The request is approved and issued by a GoldUser (a verified individual registered with the ICO and authorised to manage store data).
- The recipient is a law enforcement agency, regulatory authority, or legal representative involved in an active case.

# 8. Data Sharing & Third Parties

Footage may be shared under secure and justified conditions with:
- Law enforcement agencies (e.g., for criminal investigations)
- Insurers (for validated claims)
- Regulatory bodies (e.g., the ICO, local councils)
- Third-party processors (e.g., cloud storage providers under written agreements and compliant with UK GDPR)

# 9. Security Measures

We maintain the highest standards of data and operational security, including:
- Password-protected monitoring systems
- Encrypted video transmission
- Tamper-resistant CCTV equipment
- Role-based access to systems and footage logs

# 10. Signage and Notification

It is the responsibility of each client store to display clear and visible CCTV signage in all monitored areas. Signage must state:
- “CCTV in Operation”
- The purpose of surveillance (e.g., crime prevention, safety monitoring)
- The contact details of the data controller (e.g., the store or IntellOperations)

# 11. Individual Rights

Individuals captured by CCTV have the following rights under data protection law:
- Right of access to footage in which they are identifiable (Subject Access Request)
- Right to object to processing under certain legal grounds
- Right to lodge a complaint with the Information Commissioner’s Office (ICO)

Requests should be directed to the relevant store or to IntellOperations as appropriate.

# 12. Review and Accountability

This policy is reviewed annually or more frequently if legislation or operational practices change.

Responsibility for reviewing and enforcing this policy lies with:
hub@intellops.co.uk

# 13. Contact Information

For questions, concerns, or data-related requests, please contact:
- Customer Support: support@intellops.co.uk
- Incident Management Hub: hub@intellops.co.uk
- Billing & Administration: admin@intellops.co.uk