DUBLIN POLICE **SERVICES** **POLICY AND PROCEDURE**	**NUMBER**: 5.26	**PAGES**: 1 of 5
	RELATED ORDERS:	
	ISSUED DATE: August 21, 2018	
	REVISION DATE: N/A	
CHAPTER: Law Enforcement Operations	**SUBJECT**: DPS Situational Awareness Camera Program	

I. **INTRODUCTION:** The high-resolution, Situational Awareness Cameras (Sitcams) supplement the existing Automated License Plate Reader (ALPR) infrastructure. Sitcams have the ability to capture real-time footage of an entire area, such as a major intersection, where the cameras are installed. This will allow an intersection to be reviewed for investigative leads when a vehicle is not detected by an ALPR camera or when a vehicle does not have license plates. Sitcams also have the ability to capture criminal activity and suspect descriptions in situations when a vehicle is not involved. Depending on location and angle, Sitcams also have the ability to detect vehicle license plates, description of vehicle occupants, as well as rotate and zoom to monitor live situations. Dublin Police will utilize Hitachi Technology managed by Consiliant Technologies LLC to operate the Sitcam Program.

II. **PURPOSE:** The purpose of utilizing Situational Awareness Cameras is to equip authorized deputies and staff assigned to law enforcement roles with an effective tool to combat criminal activity, enhance productivity and improve officer safety.

III. **POLICY:**

A. Sitcams are to aid in the apprehension of criminals by identifying persons and vehicles associated with criminal activity within the City of Dublin.

B. The policy applies to law enforcement personnel assigned to Dublin Police Services and the images are collected using cameras owned and operated by the City of Dublin.

C. It is the intent of this agency to ensure that personnel utilizing Sitcams maintain reasonable security standards, procedures, and implement a usage and privacy policy with respect to the data and information obtained from said cameras. Staff shall remain cognizant of the public's concern over privacy and government intrusions.

IV. **DEFINITIONS:**

A. Consiliant Technologies LLC, founded in 2002, provides technological services including the management of Sitcam systems utilizing Hitachi products. Consiliant oversees the installation, training, maintenance and upkeep of the Sitcam system established, owned and operated by the City of Dublin.

B. Hitachi Visualization Suite (HVS): HVS provides a single web-based interface that integrates and aggregates information from disparate solutions including CCTV and edge sensors.

C. Edge Storage Solution – Solution to store captured data on the mounted Sitcams without the need for a local or cloud based data storing solution.

D. Hitachi HVP 600 SmartCam – Fixed Smart Cloud Cameras. These cameras are compact, have 4G LTE or hard wire capabilities with large edge storage capacity. The HVP 600 also has the ability to pan, tilt and zoom giving the user the customized angle of site.

E. Hitachi HVP 200 SmartCam – Fixed Smart Cloud Camera. These cameras are compact, have 4G LTE or hard wire capabilities with large edge storage capacity. The HVP 200's field of view is fixed.

V. **GUIDELINES**:

A. SITCAM USAGE

1. Sitcams may be used to collect data that is within public view, but may not be used for the sole purpose of monitoring individual activities protected by the United States Constitution. The collected data is only used for law enforcement purposes.

2. Any comments or public information requests regarding the implementation of Sitcams, will be handled by the Sitcam System Administrator or their designee.

3. The following are some situations for using the Sitcams:

a. Stolen Vehicle Identification

b. To identify wanted felons

c. BOLF's

d. AMBER Alert

e. In Progress Crimes and Investigations

f. To conduct grid searches of areas around crime scenes

g. Blue Alert

h. Silver/Gray Alert

i. Yellow Alert

j. Traffic Collision Investigations

4. Using Sitcam data shall be for official agency purposes only. Accessing the data for personal reasons, or the introduction of unapproved software, other files or altering the software program, is unauthorized.

5. Sitcam data is reviewed and accessed via the Hitachi Visualization Suite (HVS) as follows:

   a. Staff accessing the data must have a vetted HVS account establishing their ability to access law enforcement resources. To establish a HVS account staff must meet the training requirements set forth in this policy.

   b. Access to Sitcam data must be for authorized agency purposes and within “need to know right to know” guidelines. All access and inquiries to the site are logged and may be audited.

   c. Access requires a case/report number, or event number if a report number has yet to be generated.

B. DATA COLLECTION AND RETENTION:

1. Video data is stored on each individual Sitcam, utilizing the Edge Storage Solution.

2. Video data will be stored on each individual Sitcam up to 30 days. Some cameras may have a shorter retention time based on the amount of data which is captured.

3. Video data will be downloaded from the Sitcam as needed to investigate potential criminal activity.

4. Data recovered from the Sitcams and moved to a local storage solution will be stored as evidence and booked according to Alameda County Sheriff’s Office written directives.

5. Notwithstanding any other provisions of law, all electronic images or data gathered by Sitcams are for the exclusive use of law enforcement in the discharge of duties and are not to be made open to the public.

6. Outside law enforcement agencies wishing to view or copy data recovered from Sitcams will be allowed to do so at the discretion of the Chief of Police or their designee.

C. DEPLOYMENT

1. Cameras will only be placed in public areas to address issues of concern within the City of Dublin.

2. Cameras will be positioned to capture vehicle or pedestrian traffic in a way that will allow for the identification of a person or the identification of a vehicle via license plate or description.

3. Cameras will not be positioned so as to point onto someone's private property, specifically where someone holds a reasonable expectation of privacy.

D. COMPLAINTS

1. All internal and external complaints will follow standard complaint procedure as outlined in the Alameda County Sheriff's Office written directives and applicable laws.

E. SYSTEM ADMINISTRATOR

1. The Dublin Police Services Administrative Lieutenant is the Sitcam System Administrator. The System Administrator's responsibilities shall include:

   a. Training selected operators of the system and ensuring they receive periodic training as needed.

   b. Ensuring data collection and retention policies are strictly adhered to.

   c. Overseeing the maintenance of the Sitcam system.

F. TRAINING

1. The System Administrator can authorize Dublin Police staff to utilize the Sitcam system once they have been trained, showing proficiency and an understanding of operational procedures.

2. All staff wishing to access the Sitcam system shall review and sign off this policy and procedure in DMS to acknowledge they have reviewed and understand the Sitcam system and training. Staff shall not utilize the Sitcam system without first acknowledging these documents.

G. DATA BREACH:

1. In the case of any data breach/compromise of personal information contained in our Sitcam system owned or operated by Dublin Police, the following procedures are required:

   a. For breaches within our Agency, if possible, identify the breach/compromise and contact the Sitcam System Administrator or designee.

   b. The Sitcam System Administrator will notify the Office of Information Security (California Department of Technology), pursuant to reporting mandates set by state law.

   c. All affected individual(s), will be notified by the Sitcam System Administrator, via a "Notice of Data Breach" form; detailed in the form are categories which include the incident detail, information involved, remedies for the victim(s), what the Dublin Police are doing to resolve the issue, and contact information for the Dublin Police.

d. Any breach notification from an outside source, will be made using the normal police reporting guidelines (i.e., filing a report with their local law enforcement agencies). All instances will be forwarded to the Sitcam Administrator. The notification to the affected party may be delayed, if an ongoing investigation may be compromised.

e. Pursuant to Civil Code 1798.29, any victim of a computerized data breach, will be notified and advised of the breach and measures taken to fix the issue without delay.

ATTACHMENTS:

1. Sitcam “Notice of Data Breach” form.