

APPENDIX E
DOCUMENTS PROVIDED BY TRANSIT AGENCIES

Item

Ann Arbor Transportation Authority, Ann Arbor, Michigan

Electronic Monitoring, Article III, Section 3 of Union Contract 2013-2017	1
Notice of Audio/Video Surveillance	2

Antelope Valley Transit Authority, Lancaster, California

On Board Video Release Form	3
Notice of Video Surveillance in a Restricted Area	4
Notice of Video and Audio Surveillance	5

Central Ohio Transit Authority (COTA), Columbus, Ohio

Records Retention Schedule	6
DVD Surveillance Systems	7
Extracting Hard Drives from Road Recorders	8

Centre Area Transportation Authority (CATA), State College, Pennsylvania

Facility and Vehicle Surveillance Systems Policy	9
--	---

City of Detroit Department of Transportation, Detroit, Michigan

Vehicle Video Surveillance System Data Handling Procedures	10
Master Agreement between the City of Detroit Department of Transportation and Amalgamated Transit Union, AFL-CIO-Local 26, 2014-2018	11

City of Eau Claire Transit, Eau Claire, Wisconsin

City of Eau Claire Owned and Operated Cameras Policy, January 10, 2014	12
--	----

City of Gardena Municipal Bus Lines (GTrans), Gardena, California

City of Gardena, Resolution No. 6235, Establishing a Retention Policy for GTrans Video Surveillance Recordings	13
--	----

Notice of Video and Audio Observation System	14
Dallas Area Rapid Transit (DART), Dallas, Texas	
DART Police Special Order, Procedures on Release and Handling of DART Video	15
DART Police Department, Video Request Chain of Custody Form	16
DART Operations Policy/Procedure, Surveillance Video Requests	17
DART Retention Periods, Effective April 17, 2016	18
DART Camera Location Diagram	19
DART Standard Operating Procedure re Event Recorder	20
DART Surveillance Decal/Bus	21
Interior Security Camera Decal	22
DART Notice re Cameras in Use	23
Duluth Transit Authority, Duluth, Minnesota	
Duluth Transit Authority, Surveillance Video Control Policy	24
Duluth Notice re Bus Audio/Video Surveillance	25
Escambia County Area Transit, Pensacola, Florida	
Attachment re Bus Audio/Video Surveillance System to current Labor Agreement between ATU Local 1395 and Escambia County Area Transit	26
Greater Attleboro Taunton Regional Transit Authority (GATRA), Taunton, Massachusetts	
Use of Technology in Contract with ATU 1547, Article 24	27
Go Raleigh Transit (GoRaleigh), Raleigh, North Carolina	
N.C. Gen. Stat., Ch. 15A, Art. 16, Electronic Surveillance	28
Greater Cleveland Regional Transit Authority (RTA), Cleveland, Ohio	

RTA Administrative Procedures, Security Camera Procedures	29
Notices of Electronic Surveillance	30
RTA Bus Operator Handbook, Part 210, Cameras	31
Greater Peoria Mass Transit District, Peoria, Illinois	
Surveillance Camera Policy	32
Request for Review of Video	33
Hillsborough Transit Authority (HART), Tampa, Florida	
Standard Operating Procedure, Video/Audio Surveillance Procedures	34
Video/Audio Surveillance Receipt Form	35
Notice of Video and Audio Monitoring Equipment	36
Intercity Transit, Olympia, Washington	
Intercity Transit Policy-OP-5507, Managing Digital Video Recording System	37
Intercity Transit Policy-OP-5507-A, Retrieving DVR Hard Drives	38
Intercity Transit Policy-OP-5507-B, Auditing Monthly DMERS	39
Intercity Transit Task-OP-5507-A, Retaining DVR System Recorded Material	40
Intercity Transit Task-OP-5507-B, Reviewing DVR System Recorded Material	41
Intercity Transit Form-OP-5507, DVRS Master Evidence Record	42
Memorandum of Agreement, Intercity Transit and ATU Local 1384	43
Notices of Video and Audio Surveillance	44
Lehigh and Northampton Transportation Authority (LANTA), Allentown, Pennsylvania	

Video Surveillance/Camera Maintenance Policy	45
Massachusetts Bay Transportation Authority, Boston, Massachusetts	
Policy on MBTA Video Access, Distribution, & Retention	46
Video Access Request Form	47
Metropolitan Atlanta Rapid Transit Authority (MARTA), Atlanta, Georgia	
Department of Police & Emergency Management, Authority-Wide CCTV Policy	48
Metro Transit, Madison, Wisconsin	
Security Camera Surveillance Police	49
Mayor's Office, Administrative Procedure Memorandum No. 3-17 Re Use of Surveillance Cameras	50
Milwaukee County Transit System (MCTS), Milwaukee, Wisconsin	
MCTS Employee Mobile Video Surveillance System (MVSS) User Agreement	51
Monterey-Salinas Transit District (MST), Monterey, California	
Memorandum to All Employees re Electronic Monitoring Systems	52
Memorandum to All Coach Operators re Kal-A-Tel Video Surveillance System	53
Standard Operating Procedure, SEON Video Management, DVR Exchange, & Reporting Procedures	54
Pierce Transit, Lakewood, Washington	
Task Outline, TSK-11200.11, Reporting Problems with Physical Security Equipment	55
Policy, POL-1250.09, Cameras on Buses	56
Fixed & Mobile CCTV Requests	57
Rhode Island Public Transit Authority, Providence, Rhode Island	

Rhode Island Public Transit Authority Administrative Policies and Procedures, Surveillance Camera Policy	58
Santa Clara Valley Transportation Authority (VTA), San Jose, California	
CCTV Monitoring & Preserved Footage Policy	59
Request of Law Enforcement Agency for Release of Recorded Audio/Video Data	60
VTA Board Memorandum re Closed-Circuit Television (CCTV) Policy	61
Tri-Met, Portland, Oregon	
Tri-Met Security re Camera Installation/Change Request	62
Tri-Met Security re CCTV Camera Acceptance (Fixed Facilities)	63
Tri-Met Security re CCTV Video Management System User Access (Fixed Facilities)	64
Tri-Met Security re CCTV Roles and Responsibilities	65
Tri-Met Human Resources Manual, Information Technology: CCTV Use	66
Tri-Met CCTV Use Policy Receipt	67

Ann Arbor Transportation Authority, Ann Arbor, Michigan

Electronic Monitoring, Article III, Section 3 of Union Contract 2013-2017

1

SECTION 3 – ELECTRONIC MONITORING

A. Definition

Monitoring/surveillance for the purposes of this section refers to the use of instruments or machines including the collection of information concerning employee activities or communications by the use of a computer, telephone, wire, radio, video camera, audio recording devices, photo electronic or photo-optical system, proximity readers and other electronic sensing devices to observe, detect, or record activities occurring in or around all Employer owned or leased buildings, property and vehicles.

B. Purpose:

The primary function of monitoring/surveillance by the Employer is to enhance the safety, security and protection of employees, visitors, customers and physical assets of the Employer and/or Employees. Monitoring/surveillance may also be utilized on a specific case-by-case basis for reasons including:

1. To protect the Employer and employees from false or frivolous claims and accusations.
2. Any incident or accident in an AATA vehicle or at any AATA facility.
3. Any complaint received by the Employer which is being investigated by the Employer.
4. To establish the existence of facts relevant to the Employer's business, such as to record conversations over the telephone.
5. At the request of a police agency or court system when an accident/incident or criminal activity may have been captured by AATA monitoring/surveillance equipment.
6. To prevent or detect crimes.
7. To investigate or detect the unauthorized use or misuse of Employer assets.
8. To promote compliance with rules, policies, and procedures, provided the video will not be used in a random or discriminatory manner.

Any incident or situation arising that may not be covered by the language in B above will be addressed jointly by labor and management.

C. Hours

The Employer reserves the right to monitor in and around all its buildings, properties, and vehicles at any and all times.

D. Respect for Privacy

Surveillance cameras and related equipment shall not be used in employee occupied break rooms and in any other areas where employees have a reasonable expectation of privacy i.e., washrooms.

E. Discipline and Time Limits

Any discipline administered as a result of monitoring/surveillance will be issued in a manner consistent with discipline and time limit practices as defined in Article III, Section 1 A and B.

F. Disclosure

Any monitoring/surveillance documentation (such as recordings) used by the Employer to discipline an employee will be available for review by the employee and/or his/her Union representative during or following any disciplinary conference, upon request. Any non-monitoring evidence gathered in an investigation and used to corroborate monitored activities will be shared with the employee or Union representative.

G. Storage and Archiving

Information gathered in monitoring/surveillance activities shall normally be stored on hard drives and will be overwritten, unless the information has been downloaded and archived for use in

ongoing investigations, open employee grievances or at the request of legal authorities, or is intended to be used for future training purposes. Audio and video recordings of active employees will not be used for training purposes without the employee's consent. The Employer will gather all information of relevance to the employee and/or the employer captured by the video (both before the incident and after the incident occurred) before the hard drive has been placed back in service. If the involved employee feels there is information that may have been captured on AATA surveillance systems that is relevant to the matter being reviewed, he/she should advise the investigating supervisor as soon as possible. Storage and archiving of all information gathered in monitoring/surveillance shall be in a secure place with access limited to authorized personnel.

**FOR YOUR SAFETY AND
SECURITY THIS BUS MAY
BE UNDER AUDIO/VIDEO
SURVEILLANCE**

04 25 2017 17 32

Antelope Valley Transit Authority, Lancaster, California

On Board Video Release Form

3

**ANTELOPE VALLEY TRANSIT AUTHORITY
ON BOARD VIDEO RELEASE FORM**

Incident Date: _____ Time: _____

Description: _____

Route: _____ Vehicle Number: _____

Operator: _____ (if known)

Reason: _____

Length of video (minutes): ____ (max. 30 min)

I agree not to duplicate, upload or save this video in any form or release the video to any individual or company not authorized by AVTA Director of Operations or operations General Manager.

Video Media Received By:

Organization:

Printed Name: Title:

Signature: Date: Time:

=====

Authorized by (signature): Date:

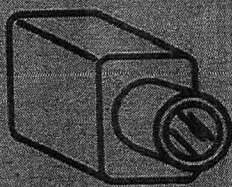
Released by: Date:

NOTE: Release of video can only be authorized by AVTA Executive Director, AVTA Director of Operations and Transdev General Manager. Personnel outside AVTA must submit a public information request in addition to executing this form. Request will be reviewed by AVTA's attorney.

RESTRICTED AREA

**NO UNAUTHORIZED
PERSONNEL
BEYOND THIS POINT**

VIOLATORS WILL BE PROSECUTED
Penal Code Section 602



**VIDEO SURVEILLANCE
IN USE ON THESE
PREMISES**

NOTICE!

VIDEO AND AUDIO SURVEILLANCE

This vehicle is equipped with an on-board surveillance system. Video and/or audio may be recorded.

ATENCION!

VIGILANCIA DE VIDEO Y AUDIO

Este vehículo está equipado con un sistema de vigilancia de video y audio. Video y/o audio pueden ser grabados.



Central Ohio Transit Authority (COTA), Columbus, Ohio

Records Retention Schedule

Records Retention Schedule for the Central Ohio Transit Authority

[illegible]

Record or Record Series ¹	Retention Period
Fringe Benefit Analysis Report	Current + 3 years
General Correspondence ²	6 months ²
General Ledger	Current + 3 years
GFI Reports	Current + 10 Years
GO-Proof Equipment Edits	Current + 10 years
Health Claim Checks	Current + 3 years
Huntington/Star Banking Records	Current + 3 years
Inventory Reports	Current + 3 years
Journal Entries	Current + 3 years
Liability Self-Insurance Report	Current + 4 years
Longevity Records	Current + 10 years
Mileage Reports	Current + 3 years
Monthly Financial Reports	Current + 3 years
Motor Fuel Tax Returns	Current + 7 years
Operating Summary Report	Current + 5 Years
Paratransit Report	Current + 5 Years
Passenger Ridership Report	Current + 5 Years
Payables/Events/Bonds	Current + 10 years
PERS	Permanent
Purchase orders/Check Requests	Current + 5 years
Quarterly/YTD Registers	Current + 10 years
Revenues & Expenses Summary	Current + 5 years
Special Services Report	Current + 5 Years
Transient Documents	Discard when no longer of administrative value
Uniform/Tool	Current + 10 years
Union Dues Records	Current + 10 years
Voided Checks	Current + 3 years
Weekly Management Report	
Z-Tapes	Current + 3 years
Audit Work Papers	Permanent
Procurement Card Reports	Current + 3 years
Expense Reimbursement Info	Permanent
Procurement	
Contract Files	Active + 16 years
General Correspondence ²	6 months ²
Davis-Bacon Act	Current + 3 years
Executive Order 11245	7 years
Fee Simple Property Files	21 years after property disposition
Leases of Owned Property	Active + 10 Years
Leased Facilities	Active + 10 Years
Purchasing Policies and Procedures	Active + 16 Years
POs	Current + 5 years
Proposals submitted by vendors	Sale of goods 5 years, services 16 years
RFB/RFP files	Sale of goods 5 years, services 16 years
Vietnam Era Veterans' Readjustment Assistance Act	One year by contractor
Check Request Forms	Current + 3 years
Inventory Records	Current + 2 years
Bid Files	Active + 18 years
Bid Quotes	Active + 16 years
Records Retention	Permanent
Transient Documents	Discard when no longer of administrative value
General	
Cancelled Grant Checks	Active + 3 Years after completion of Project Expenditure Submission & Audit
Federal Operating Assistance	Active + 3 Years after completion of Project Expenditure Submission & Audit
Grant Applications not approved	2 years
Grant Closing	Active + 3 Years after completion of Project Expenditure Submission & Audit
Grant File	Active + 3 Years after completion of Project Expenditure Submission & Audit
Grant Management Files	Active + 3 Years after completion of Project Expenditure Submission & Audit
Grant Purchase Orders and Requisitions	Active + 3 Years after completion of Project Expenditure Submission & Audit
ODOT Operating/Capital Assistance App.	Active + 3 Years after completion of Project Expenditure Submission & Audit
Operating Assistance Grants Section 5	Active + 3 Years after completion of Project Expenditure Submission & Audit
Operating Assistance Grants Section 9	Active + 3 Years after completion of Project Expenditure Submission & Audit
Property Depreciation files	Active + 3 Years after completion of Project Expenditure Submission & Audit
Request for FTA funds	Active + 3 Years after completion of Project Expenditure Submission & Audit
Transient Documents	Discard when no longer of administrative value
Triennial Review	Permanent
Sales	
JV's (daily deposits)	Current + 3 years
Kiosks Agreements	Current + 3 years
Lost & Found records	Current + 1 year
Outlet Consignment Agreement forms	Current + 16 years
Outlet Consignment Reports	Current + 16 years
Overage/Shortage Reports	Current + 3 years
Pass Inventory Reports	Current + 3 years
Pass Reconciliation Reports	Current + 3 years
Transient Documents	Discard when no longer of administrative value
Change Request Forms	2 Years
Payroll	
Cancelled Checks	10 years
Deferred Compensation Report	10 years

Record or Record Series ¹	Retention Period
Garnishments	10 years
General Correspondence ²	6 months ²
Operator's Payroll Hours Report	10 years
Overtime Analysis Report	10 years
Misc. Payroll Info	10 years
Payroll Checks Cancelled	10 years
Payroll Deductions	10 years
Payroll Journal	10 years
Payroll Time and Attendance	10 years
PERS Payments	10 years
Personnel Records	Current + 60 years
Salary Payroll	Current + 10 years
Time Cards	Current + 10 years
Timecards - Board	Current + 10 years
Timecards - Maintenance	Current + 10 years
Timecards - Operators	Current + 10 years
Timecards- Admin	Current + 10 years
Timecards- Equipment	Current + 10 years
Timecards- Fields/McKinley	Current + 10 years
Timecards- GO	Current + 10 years
Transfer Requests Payroll	Current + 10 years
Transient Documents	Discard when no longer of administrative value
Vacation/Sick Reports	Current + 10 years
W2 Reports	Current + 10 years
W2 Statements	Current + 10 years
W4 Statements	Current + 10 years
Weekly Payroll Totals	Current + 10 years
Petty Cash Records	Current + 3 years
Information Technology	
Consultant Reports	Current + 3 years
Departmental Budgets	Current + 3 years
Electronic Mail (Authority wide)	One month
Electronic Mail (Backups)	Rotated every four weeks
General Correspondence ²	6 months ²
Internet Access History	45 Days
MAGIC Records	Permanent
Network Shares and Databases	12 backup cycles
Personnel Records	Permanent
Phone Mail Messages (Backups)	1 Month
Project Files	Current + 5 Years
Software CD's	For the life of product
Terminated Employee Data	Backed up upon termination. Documents and data should be reviewed by supervisor and
Transient Documents	Discard when no longer of administrative value
Human Resources and Labor Relations	
Office of the Vice President	
Compensation Plan	Current + 10 Years
Employee Handbook	Permanent (A copy of each revised/rescinded policy should be maintained.)
Policies and Procedures	Permanent (A copy of each revised/rescinded policy should be maintained.)
General Correspondence ²	6 months ²
Organizational Charts	Permanent (A copy of each revised/rescinded org chart should be maintained.)
Job Descriptions	Current + 7 years
Job Evaluations (CPQ and resulting rating sheets)	Current + 7 years (kept with the corresponding Job Descriptions)
Personnel File	Permanent
Transient Documents	Discard when no longer of administrative value
EEO	
Employment Applications + Resumes + Test Results	7 years
Resumes in response to ads - No application	2 years
Unsolicited resumes but related to current COTA position	2 years
Unsolicited resumes and unrelated to COTA position	30 days
EEO Quarterly Reports	7 years (First 3 years must be a COTA administrative offices)
General Correspondence ²	6 months ²
H1-B	One Year beyond last date on which any H-1B nonimmigrant is employed under LCA or if no nonimmigrants were employed, one Year from date the LCA expired or was withdrawn
Immigration Reform & Control Act (INS Form I-6, Employment Eligibility Verification Form)	Three Years after date of hiring or one Year after date of employee's termination whichever is later.
Job Postings	7 years
Position Requisitions	7 years
Title VII	10 years
Transient Documents	Discard when no longer of administrative value
Training³	
Basic Training Records	Current + 10 Years
CDL Training	Current + 10 Years
Training Materials	Current + 10 Years
Training Sign In Sheets	2 years
Training Attendance Records	Current + 10 Years
General Correspondence ²	6 months ²
Transient Documents	Discard when no longer of administrative value
Tuition Reimbursement	Current + 5 Years

Record or Record Series ¹	Retention Period
Employee and Labor Relations	
ADA	7 years
COBRA	Current + 10 years
EEO	7 years (First 3 years must be a COTA administrative offices)
Employee Benefits File	Permanent
Employee Recognition	Permanent
Fitness/Wellness Program Receipts	3 years
FMLA	Current + 3 years
FLSA Determinations	Current + 7 years (Kept with the corresponding Job Descriptions)
General Correspondence ²	6 months ²
Health Insurance (HIPPA)	7 years
PERS	Permanent
Arbitration Awards	Permanent
Grievances	Permanent
Labor Contracts	Permanent
Miscellaneous MOA and Settlements	Permanent
Negotiations	Current + 16 years
OBES	Permanent
Transient Documents	Discard when no longer of administrative value
Union-Management Meeting Minutes	Permanent
Risk	
Emergency Action Plan	Until superseded
Environmental Testing Report	30 years
General Correspondence ²	6 months ²
Hazard Communications	30 Years
Hazard Material Spill	30 Years
Hazardous Materials List by Vendor	Current + 3 years
Hazardous Waste Contracts	16 years after expiration
Documentation of refusals to take required drug or alcohol test	6 years
Covered employee referrals to the substance abuse professional	6 years
Copies of annual MIS reports submitted to FTA	6 years
Verified positive drug test results	6 years
Negative drug test results	2 years
Records related to the drug and alcohol testing collection process	3 years
Records related to drug and alcohol awareness employee training	3 years
OSHA	5 years
Insurance Policies	16 years after expiration
Liability Insurance Policies	16 years after expiration
Transient Documents	Discard when no longer of administrative value
Workers Compensation	
Employee Accident Report	7 years after separation
Employee Injury and Lost Time Summary	7 years after separation
Employee Injury/Lost Time Summary - Detail	7 years after separation
General Correspondence ²	6 months ²
Transient Documents	Discard when no longer of administrative value
Workers' Comp Claims - Lost time	7 years after separation
Workers' Comp Claims - Medical	7 years after separation
Legal & Government Affairs	
Claims	
Accident Recommendation Log	25 Years
Accident/Incident Reports - Database	Permanent
Accident/Incident Reports - Monthly Listing	Current + 3 years
Claim Files	8 years after case closes or 6 years after SOL for Hard Copies / Electronic system
Claim Files, Minors	8 years after case closes or 6 years after age of majority for Hard Copies / Electronic
Collision and Passenger Accident Summary	Current + 6 Years
General Correspondence ²	6 months ²
Incident Reports	6 years
Major Accident Files	8 years after case closes or 6 years after SOL-age of majority for Hard Copies /
Month End Reports	Current + 6 years
Transient Documents	Discard when no longer of administrative value
Government Affairs	
JLEC Reports	3 years
Legislation / Lobbying documents	Current + 5 years
Transient Documents	Discard when no longer of administrative value
Legal	
ADA Files	7 years after case closed
Arbitration Case Files	7 years after case closed
Arbitration Decisions	Permanent (in HR)
Audit Files	Current + 3 years (in Finance)
Collections - Contract / Tuition	3 years after claim closes or 2 year after SOL
Contracts	Active + 16 years
Employee Investigation Files	7 years after separation
Employee Legal Files (settlements, FMLA etc)	7 years after separation
Ethics Commission Financial Disclosure Statements	
General Correspondence ²	6 months ²
General Finance Files	Current + 3 years
Lawsuit/Litigation Files	5 years after all appeals are exhausted
Lawsuit/Litigation Files, Minors	5 years after age of majority

Record or Record Series ¹	Retention Period
Leases of Owned Property	Active + 10 Years
Leased Facilities	Active + 10 Years
Legal Requests	2 Years
Levy files / Election info	20 years
Legal Division Policies and Procedures	Permanent. A copy of each policy that is updated, amended or superseded should be maintained.
Project Files	Current + 3 years
Public Records Request	3 years
PURTRCB Certificates of Assurance	Permanent
Transient Documents	Discard when no longer of administrative value
SERB Files	Active + 10 years
Operations	
Office of the Vice President	
Division Budget	Current + 3 years
Leadership Team (senior management) meeting information	Current + 2 Years
General Correspondence ²	6 months ²
Grievance Information	Permanent
Individual PMP's	Current + 3 years. Copies only - Originals are maintained by HR as part of the personnel
MIMS requisitions	Current + 3 Years
Resolutions	2 years - Copies only - Originals are maintained by President's Office.
Special project files	Current + 3 years
Transient Documents	Discard when no longer of administrative value
Union Correspondence*	Current + 5 Years
McKinley and Fields Bus Operations	
Accident/Incident Forms	5 years
Accident/Incident Report-Monthly Listing	5 years
Attendance Record Computer Generated	Current + 3 years
BMV Quarterly License Check	Current + 3 years
Cleanliness Report	90 days
Daily Radio Supervisor Report	Current + 3 years
Daily Report Cards	Current + 3 years
Daily Transportation Report	Current + 3 years
Emergency Telephone List	Until superseded
Employee Awards Program	7 years after separation
Employee Master File	3 years in Transportation then coordinate with HR to maintain with HR Personnel Records
Federally Funded Projects	Active + 3 Years after completion of Project Expenditure Submission & Audit
General Correspondence ²	6 months ²
Grievances	Permanent
Hard Copies of Logs	2 years
Job Description	7 years
Job Posting	7 years
Lost and Found List	Current + 3 years
Lost and Found Claim Check	Current + 3 years
Manifests	Current + 3 years
Maintenance Records	Life of the vehicle
Monthly Reports	Current + 3 years
Monthly Mileage Report	Current + 3 years
Operator Route Book	Current + 3 years
Payroll/Time & Attendance	Current + 10 years
Personnel Telephone	Until superseded
Pick Schedule - Check w/Ginny	1 year
Policies & Procedures (Transportation)	Current + 3 years
Portable Radio/Camera/Equip Sign-out Sheet	Current + 3 years
Project Work Papers	Current + 5 years
Quarterly Review	Current + 3 years
Radio Log	Current + 3 years
Request for Birthday/Personal Holiday	Current + 3 years
Reroutes	1 year
Rider/Check	3 years after completion of the project
Seniority List	Current + 1 year
Transient Documents	Discard when no longer of administrative value
Voice Tapes	1 year
Weekly Supervisor Work and Assignment Lists	Current + 3 years
Maintenance	
Employee Record Files	3 years in Transportation then coordinate with HR to maintain with HR Personnel Records
Fields Main, Closed Bus Work Orders/Inspections	Three years after disposal/transfer of vehicle
Maint./Fac. Daily Work Order Time Cards	3 years in Transportation then coordinate with HR to maintain with HR Personnel Records
General Correspondence*	6 months*
MCK/FLDS Daily time Memos	3 years in Transportation then coordinate with HR to maintain with HR Personnel Records
MCK/FLDS MIMS Payroll Interface Report	3 years in Transportation then coordinate with HR to maintain with HR Personnel Records
McKinley Main, Closed Bus Work Orders/Inspections	Retain during vehicle ownership
Transient Documents	Discard when no longer of administrative value
Vehicle Maint. End of Month Reports	Three years after disposal/transfer of vehicle
Vehicle Maint. PM Schedules	Three years after disposal/transfer of vehicle
Vehicle Maint. Road Call Reports	Three years after disposal/transfer of vehicle

Record or Record Series ¹	Retention Period
Security	
Police and other Incident Reports	5 years
Theft Reports	5 years
Visitor and Employee Log / Badge Log	1 year
SAR - Shift Activity Report	1 year
Security Officers Incident Reports	Current + 3 years
Timesheets for security	4 years
Camera of front desk	Until recorded over.
Saved Videos of Incidents & Accidents	3 years after case closed or 2 year after SOL
Issued Tickets	Current + 3 years
False Alarm Reports	2 years
Memos to guards	Current + 3 years
Emergency Response Plan	Until superseded
Security Awareness Presentations	Current + 3 years
Special Deputy Pay Log	4 years
Transient Documents	Discard when no longer of administrative value
Video from cameras on buses and facilities	Until recorded over.
Paratransit	
General Correspondence ²	6 months ²
Transient Documents	Discard when no longer of administrative value
COTA Paratransit Operator Manifests	15 years
Terminated ADA eligible customer records	7 years
Unresponsive customer's application	7 years
Planning & Scheduling	
Office of the Vice President	
CIT's files / OIP files	Active + 3 years
Communication plan files	Active + 3 years
Completed small check requests	Active + 3 years
Contract files [Purchasing]	Active + 16 years
Department Budgets	Current + 4 years
Department files	Current + 5 years
Department Goals	Current + 3 years
Division Goals	Current + 3 years
General Correspondence ⁴	6 months ⁴
Individual PMP's for entire division	Current + 3 years
Meeting notes and minutes	3 years
MIMS requisitions	Current + 3 years
Project files	Current + 5 years
Ridership reports/analysis	5 years
Transient Documents	Discard when no longer of administrative value
Transit Center files	18 years
Planning	
901 Bus Stop File and Records	Current + 7 years
Agendas, Minutes from Community Groups Meetings	Current + 7 years
Division and Department Strategic Plans	Current + 3 years
Misc. State and Federal Grant Programs	Active + 3 Years after completion of Project Expenditure Submission & Audit
General Correspondence ²	6 months ²
MORPC, TAC and CAC Agendas	No minimum
National Transit Database Report	Current + 15 years
North Corridor Light Rail	Permanent
On/off Counts, Max. Load Data, Passenger Surveys	Current + 5 years
Personnel Files	7 years - should be in HR
Productivity Analysis for Fixed Route	Current + 7 years
Survey, Counts, Realignment - Routes	Current + 7 years
TIP	Current + 7 years
Title VI Report	Current + 7 years
Transient Documents	Discard when no longer of administrative value
Triennial Reviews	Permanent
Scheduling/Service Planning	
Arbitration Materials	Permanent
Board of Trustee Meeting Information	2 years
Budget Files for Department	Current + 3 years
Bus Operator Vacation Calculation & Sign Up Sheets	Current + 3 years
DLZ - Timetable Map Changes	Current + 1 year
Extra board Operator Days Off - All related information	Current + 2 years
General Correspondence ²	6 months ²
Internal Memorandums	Current + 3 years
Line by Line files	Current + 7 years
Long Range Plan Information	Current + 10 years
Misc. Service Files (Ohio Dominican, Arena District, Downtown Hotels, etc.)	Current + 3 years
Miscellaneous Maps	No minimum
Miscellaneous Outside Studies	Current + 5 Years
Motor Coach Operator Seniority Reports	Current + 1 year
Municipality Income Tax Calculations & Memo	Current + 4 years
Off Site Storage Logs	Permanent
Operator Comments	1 year
OSU Service Related Information	Current + 5 years
Paddle Corrections	Current + 3 years
Paving the Way	Current + 5 years
Projected Service Hours	Current + 3 years

Record or Record Series ¹	Retention Period
Reroutes	Current + 1 year
Ride Checks & Point Checks	Current + 1 year
Ridership Data	Current + 5 years
Schedules for Schedule Checker Assignments	Current + 3 years
Scheduling Committee	Current + 2 years
Service Change Database	Permanent
Section 15 – NTD Reports	Current + 3 years
Service Change – Bus Pullout Reports	Current + 7 years
Service Change – Miscellaneous Info	Current + 7 years
Service Change – Operator Paddles	Current + 7 years
Service Change – Public Meeting Comments	Current + 7 years
Service Change – Roster of available Regular Operator Days Off	Current + 7 years
Service Change – Sign Up Dates & Operator Day Off Periods	Current + 7 years
Service Change – Trip Sheets & Trip Sheet Info Books	Current + 7 years
Service Change Information, Folders & Reports	Current + 7 years
Service Change Operator Sign Up Info	Current + 7 years
Service Day Calendars	Current + 7 years
Short Range Transit Plan	Current + 5 years
Special Demonstration Projects (MCi Coaches, etc.)	Current + 3 years
Special Service Files (RWB, Zoo Widelights, First Night, etc.)	Current + 3 years
System Map Files	Current + 3 years
Timetable Files	Current + 7 years
Transient Documents	Discard when no longer of administrative value
Travel Files	Current + 3 years
Union Negotiation Materials	16 years
Vehicle Fleet Spare Ratio	Current + 3 years
Capital Project Development	
Board of Trustees Info	2 years
Capital Projects	16 years after completion of the project
Expense Reports, MIMS, Smart Data	Current + 3 years - Copies only. Originals should be maintained by Finance
Forms	Current + 3 years
Lease Proposals	2 years after receipt of proposal if not accepted. If proposal is accepted and lease is executed, maintained with Lease file in Purchasing for 10 years after lease is terminated.
Office Equipment Inventory	Current + 3 years
Office Suppliers	Current + 3 years
Resources	Current + 3 years
Security	Current + 3 years
Transient Documents	Discard when no longer of administrative value

NOTES

¹ Specific documents may not appear by name but may be included in a particular type or classification of document listed. Consult with the Legal & Government Affairs Division if you have questions about the retention period of any document.

Because of the diversity of types of records maintained by COTA, it is unrealistic to anticipate any one person can practically oversee the creation and management of all COTA records. Consequently, the Administrative Assistant to the President/CEO is the custodian of records for the President's Office and the Vice President of each division has been determined to be the custodian of records unique to their respective division. For example, the V.P. of Legal & Government Affairs is the custodian of law suits, personal injury claims, lobbying records, etc., while the VP of Human Resources is the custodian of records for personnel files including PMPs, training records, etc. for personnel in the Legal & Government Affairs Division. Consistent with this approach, the custodian of records for contracts (and bids, proposals and related documents) with COTA's outside law firms is the VP of Finance as Purchasing, which is responsible for procuring goods and services from outside firms, is a department in the Finance Division.

Copies of documents may be maintained by any COTA employee for any number of reasons, however, the custodian of records should maintain the original documents. Refer any questions about the appropriate custodian of records for any document or classification of documents to the Legal Division.

² General correspondence [unrelated to any matter requiring a longer retention period] need only be retained for the stated period. Other correspondence related to a specific matter should be maintained consistent with the retention schedule for documents related to that matter.

³ The records in listed under Human Resources/Training are general training documents, not individual employee training records. Records documenting individual employees' training should be maintained as part of the employee's personnel records.

Revised 3/24/2010

DVD Surveillance Systems

PURPOSE

COTA Security and Legal Policies do not allow the unauthorized copying of Facility and Motor Coach Surveillance Systems or its film history at any time except where required by law and proper documentation is presented. This policy does not in any way over-ride any copyright protections presented by the Owner/ Dealership of "Safety Vision, Inc."

This SOP establishes procedures that will be followed and who contacted in the event the Columbus Division of Police, a Civil Attorney or other members of Trans Worker Union, Local #208 request copies of any DVD documentation from a COTA Surveillance System (Facility/Motor Coach).

GOAL

- ◇ To provide safe, clean and reliable service to all employees and passengers of the Central Ohio Transit Authority (COTA).
- ◇ To establish guidelines for safe-guarding evidence involving criminal or legal video documentation.
- ◇ Assisting local Law Enforcement Agencies in their investigations and solving major crimes.

COPYRIGHT PROTECTION

DVD Software as required to view images from COTA Facility and Motor Coach Surveillance Systems is protected through "Safety Vision (Motor Coach)" and "Vicon (Facilities)" company trademark patents. COTA will not violate any copyright laws.

SUBPOENA

A request for DVD documentation made pursuant to a subpoena will be honored.

- Upon receiving a copy of the court issued subpoena, the Director, Security or Security Investigator will provide a copy of the specific date, time and tape if it is available and viewable.
- Subpoena must be presented through the COTA Legal Department to the Security Department (COTA Security Department will not accept subpoena directly).
- Members of COTA Security Department will report to court with laptops to view any subpoena related video or DVD documentation as required by law.

PUBLIC RECORD REQUEST

All Public Record Request will be presented to the COTA Legal Department and responded to on a case by case basis.

Extracting Hard Drives from Road Recorders

PURPOSE

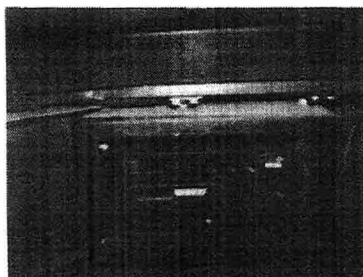
To establish one procedure for extracting Hard Drives from Safety Vision Road Recorders.

GOAL

- ◇ Ensure that Hard Drives (tapes) are extracted properly from the Road Recorder.
- ◇ To ensure that there is a valid reason for the Hard Drive to be extracted.
- ◇ Provide knowledge on the different models of Road Recorders in service on COTA Coaches.
- ◇ COTA employees that are authorized to extract Hard Drives and the Proper COTA Employee to turn the Hard Drive in to.
- ◇ Ensure footage and the Hard Drives are not damaged.

POLICY

The Road Recorder 5000 is the oldest model and is on most of the COTA Coaches. The lock box in which the Road Recorder is secured in is called a NEMA Box which shelters the Road Recorder from damage and misuse to the equipment. When attempting to extract a Hard Drive from the RR 5000 follow these instructions:



ROAD RECORDER 5000

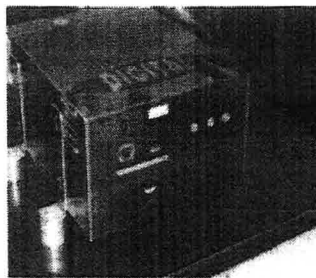
1. Unlock the Nema Box with your CH751 key issued through the Security Department.
2. Look at the two lights located to the right and atop of the key insert. Before extracting the Hard Drive make sure that the top light is green and the right side light is flashing red. This indicates that the Hard Drive and Road Recorder are in working order.
3. Using your Road Recorder key issued by Security insert and turn the key to the right. On the Road Recorder it is printed REMOVE. Your key should be positioned toward this marking.
4. Wait for the top light to start flashing red; if you do not wait for this you risk damaging the Hard Drive and the footage.
5. Once the top light is flashing red you may extract the Hard Drive.
6. After extracting the tape make sure to replace it with another 5000 Hard Drive. If you are not in possession of a spare 5000 HD see the Security Investigator (Amanda Brooks 275-5820) and/or the Accident Investigator (Yvette Elkins 298-2303).
7. Once you have replaced the 5000 Hard Drive turn the key to the left; on the Road Recorder it states RUN.

Extracting Hard Drives from Road Recorders

Once the key is in that position wait for the top light to turn green and the right light to a flashing red. This indicates that the system is in working order.

8. The Hard Drive is only to be turned into the appropriate COTA Employee: Director, Security, Security Investigator, and/or Accident Investigator.

The Road Recorder 6000 is an updated version of the Road Recorder and is being installed on all new coaches. The Road Recorder 6000 hard drive is a little different than the 5000. The 6000 Hard Drive will sometimes state 6000 Hard Drive but at the bottom of the hard Drive is a round inserted knob. Note: It is important to not insert a 5000 HD in a 6000 RR. The system will not work and no footage will be recorded. When attempting to extract a 6000 HD follow these instructions:

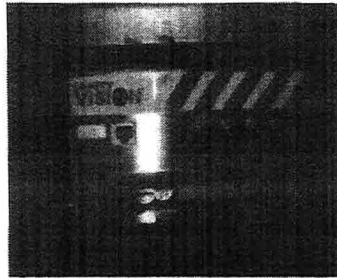


ROAD RECORDER 6000

1. Unlock the Nema Box with your CH751 and/or Y11, Y12 key issued through the Security Department.
2. Look at the two lights located to the right and atop of the key insert. Before extracting the Hard Drive make sure that the top light is green and the right side light is flashing red. This indicates that the Hard Drive and Road Recorder are in working order.
3. Using your Road Recorder key issued by Security insert and turn the key to the right. On the Road Recorder it is printed REMOVE. Your key should be positioned toward this marking.
4. Wait for the top light to start flashing red; if you do not wait for this you risk damaging the Hard Drive and the footage.
5. Once the top light is flashing red you may extract the Hard Drive.
6. After extracting the tape make sure to replace it with another 6000 Hard Drive. If you are not in possession of a spare 6000 HD see the Security Investigator (Amanda Brooks 275-5820) and/or the Accident Investigator (Yvette Elkins 298-2303).
7. Once you have replaced the 6000 Hard Drive turn the key to the left; on the Road Recorder it states RUN. Once the key is in that position wait for the top light to turn green and the right light to a flashing red. This indicates that the system is in working order.
8. The Hard Drive is only to be turned into the appropriate COTA Employee: Director, Security, Security Investigator, and/or Accident Investigator.

Extracting Hard Drives from Road Recorders

The Road Recorder 6000 5C is our latest addition, it is being installed on coaches where the 5000 RR are no longer functional. The RR 6000 5C is almost the same as the RR 6000 but it does not have some of the features the RR 6000 has. The RR 6000 5C does require a 6000 HD. Note: It is important to not insert a 5000 HD in a 6000 RR. The system will not work and no footage will be recorded. When attempting to extract a 6000 HD follow these instructions:



ROAD RECORDER 6000 5C

1. Unlock the Nema Box with your CH751 and/or Y11, Y12 key issued through the Security Department.
2. Look at the two lights located to the right and atop of the key insert. Before extracting the Hard Drive make sure that the top light is green and the right side light is flashing red. This indicates that the Hard Drive and Road Recorder are in working order.
3. Using your Road Recorder key issued by Security insert and turn the key to the right. On the Road Recorder it is printed REMOVE. Your key should be positioned toward this marking.
4. Wait for the top light to start flashing red; if you do not wait for this you risk damaging the Hard Drive and the footage.
5. Once the top light is flashing red you may extract the Hard Drive.
6. After extracting the tape make sure to replace it with another 6000 Hard Drive. If you are not in possession of a spare 6000 HD see the Security Investigator (Amanda Brooks 275-5820) and/or the Accident Investigator (Yvette Elkins 298-2303).
7. Once you have replaced the 6000 Hard Drive turn the key to the left; on the Road Recorder it states RUN. Once the key is in that position wait for the top light to turn green and the right light to a flashing red. This indicates that the system is in working order.
8. The Hard Drive is only to be turned into the appropriate COTA Employee: Director, Security, Security Investigator, and/or Accident Investigator.

Note: Hard Drives are not too be extracted from a COTA Coach unless it is in reference to an Accident, Security Incident and/or a Legal Reason.

Extracting Hard Drives from Road Recorders



Procedure

SEP029.01

Revision Date: 11.20.12

Page 4 of 4

Authorized COTA Employees: The following Employees are authorized to extract Hard Drives from the Road Recorders.

Director, Security:

W. Stan Alverson
614-275-5827

Transportation Service Supervisors

Accident Investigator:

Yvette Elkins
614-298-2303

Security Investigator:

Amanda L. Brooks
614-275-5280

All Hard Drives that are extracted are to be turned into the following authorized COTA Employees:

Director, Security:

W. Stan Alverson
614-275-5827

Accident Investigator:

Yvette Elkins
614-298-2303

Security Investigator:

Amanda L. Brooks
614-275-5280

Report all damage, missing Hard Drives and systems that are not functioning properly to the Security Investigator (Amanda L. Brooks 614-275-5280 brooksal@cota.com) or the Accident Investigator (Yvette Elkins 614-298-2303 elkinsym@cota.com).

Centre Area Transportation Authority (CATA), State College, Pennsylvania

Facility and Vehicle Surveillance Systems Policy

CATA

FACILITY AND VEHICLE SURVEILLANCE SYSTEMS POLICY

CATA places the highest priority on employee, passenger and public safety. Placing video cameras on CATA vehicles and in CATA facilities is one way to enhance employee and passenger safety, proper driver management and general security of resources for the authority.

Postings

CATA will post notices on each vehicle where cameras are located, which specify that cameras are pulling both audio and video.

Ownership of Videos

The ownership of video files from CATA vehicles and facilities rests exclusively with CATA.

In the case of accident investigations and/or criminal investigations, CATA may provide video files to its solicitor, insurance adjuster and other persons who may require the use of such video.

Nothing in this description should be construed to provide additional rights as to the review and/or duplication of video files under the Pennsylvania Right to Know Act. Any and all exceptions as to the review and/or duplication of files under the Right to Know Act remain applicable to all video files.

Viewing

CATA may view video from the cameras for any reason including performance reviews of drivers, accident investigation, investigation of passenger and/or driver complaints, camera maintenance and/or testing, criminal investigation purposes or other reasons determined by CATA as to the necessity to review video files.

CATA may use vehicle and/or property cameras and video as a method of cooperating with law enforcement personnel to investigate accidents, crimes or other activities upon request by a law enforcement officer.

CATA does not monitor cameras on an on-going basis.

Video Retention

In the event of accident or criminal investigation retention, such video files will be retained for a period of three years after the event, or until such time as litigation has come to an unappealable resolution. In the event that a video file is retained for any other purpose, CATA will refer to its record retention schedule.

Video files will be retained in a manner that protects any digital video format based upon the technology available at CATA.

Otherwise, video files are overwritten approximately every 30 days.

Maintenance

The video surveillance and DVR systems will be maintained according to the procedures outlined in the CATA facilities and equipment maintenance program.

Operators or maintenance personnel will report malfunctioning cameras immediately, in writing, to the maintenance department.

CATA will not make a practice of checking cameras on daily pre-trip and/or post-trip inspections.

CATA will make reasonable effort to ensure that its cameras are operational. However, due to the mechanical nature of cameras, CATA cannot guarantee the operation of one or more vehicle or facility cameras at any given time.

Adopted 11-28-16

City of Detroit Department of Transportation, Detroit, Michigan

Vehicle Video Surveillance System Data Handling Procedures

10

Vehicle Video Surveillance System Data Handling Procedures



Detroit Department of Transportation
1301 East Warren Avenue
Detroit, Michigan 48207
Telephone: 1(313) 833-7679

Table of Contents

Revision Control	2
Request/Chain of Custody Procedure	3
Purpose	3
Scope	3
Definitions	3
Responsibilities	3
Procedures	3
Request/Chain of Custody Form	4
Instructions for Use of the Request/Chain of Custody Form	5
Request/Chain of Custody Details	5
Data Retrieval Authority Procedure	6
Purpose	6
Scope	6
Definitions	6
Responsibilities	6
Procedures	6
Data Request Handling Procedure	8
Purpose	8
Scope	8
Definitions	8
Responsibilities	8
Procedures	8
Data Retention and Destruction Procedure	10
Purpose	10
Scope	10
Definitions	10
Responsibilities	10
Procedures	10
Vehicle Video Maintenance Responsibilities and Procedures	13
Purpose	13
Scope	13
Definitions	13
Responsibilities	13
Procedures	14

Revision Control

When any part of this Chain of Custody (COC) procedure requires amendment, the document shall be reissued in its entirety; requests for change shall be addressed to Management Information Services (MIS) and the VVS Administrator.

Revision	Date	Change Description	Originator(s)
000	11/14/13	New	P. Tacy

Request/Chain of Custody Procedure

Purpose

This Request/Chain of Custody procedure is intended to help Detroit Department of Transportation (DDOT) employees and representatives to determine what tasks to follow when retaining Vehicle Video Surveillance (VVS) data for evidence. Any employees with questions regarding this procedure should go see their supervisor.

Scope

This document covers the procedures for handling VVS data that may be used as evidence.

Definitions

VVS hardware will be defined as Mobile View Digital Video Recorder (DVR) and removable Hard Drive (Data Storage). Recording cannot proceed unless the DVR locking cover to the hard drive is in place.

Major Incidents will be defined as an accident where someone lost their life, a serious injury, or a criminal occurrence where the authorities had to respond to the scene of the crime.

Responsibilities

MIS and DDOT Security Administrator (Security) will be responsible for ensuring that the data retrieval process is followed, especially the completion and review of the Request/Chain of Custody Form.

MIS will be responsible for the handling/transport of DVR and Data Drives.

In extenuating circumstances, namely major incidents, **Transit Police (Deputy Chief Dwayne Love or designee), or the Director** will be responsible for the handling/transport of this equipment between the vehicle and data center. **MIS will provide adequate training on how to retrieve a hard drive from a vehicle and replace hard drives into vehicles.**

If the Detroit Police Department is on the scene of a serious incident that involves one of our vehicles and requests a hard drive at the scene, Deputy Chief Love or designee will be responsible for removing the hard drive and advising the Detroit Police Department representative that all hard drives and video will only be released at the data center after the proper Chain of Custody Form (COCF) is completed.

MIS will analyze all data from our systems/drives before any video is disseminated. Once the COCF is completed, it will follow the evidence until it is released. After releasing the video, the COCF will be filed in the designated filing room for five (5) years from the date of original filing. After the life span is expired, all video or drives will be destroyed by the Detroit Transit Police with a burn or shredding. An itemized report of burned or shredded video will be completed and submitted to Manager

Bernadette Williams.

If the Detroit Police Department requests video or to review video from one of our systems, the requesting member shall have the rank of Commander or above unless another person is identified and mutually agreed upon by the Detroit Police Department and the Detroit Transit Police. The requesting member from the Detroit Police Department will contact Manager Bernadette Williams for such a request. Manager Williams will confer with Deputy Chief Love and once they both agree, the video will be made available for review or dissemination.

DDOT MIS, Security, Director, and Transit Police will be responsible for re-evaluating this procedure and form on an annual basis or when a revision to the existing VVS infrastructure is made that requires changes.

Chain of Custody Process

The Request/Chain of Custody Form is shown below followed by instructions details, and procedural requirements.

Request/Request/Chain of Custody Form

STAFF/CITIZEN REQUEST	Basis of Request:	Data Requested Format (i.e. DVR, *.avi, *.wmv):	Bus No.:	Required Point of Contact (POC):	POC Phone Number:	POC Phone Number:
	Scope of Request, Include Type of Incident, Location, and Description, Including Date/Start Time and End Time of Recording Needed:					
INTERNAL USE ONLY	Request Approved By:	Date	Time	Request Completed By:	Date	Time
	Approval Notes:			Request Completion Notes:		
CHAIN OF CUSTODY	Relinquished by	Date	Time	Received by	Date	Time
	Relinquished by	Date	Time	Received by	Date	Time
	Relinquished by	Date	Time	Received by	Date	Time
	Relinquished by	Date	Time	Received by	Date	Time
	Relinquished by	Date	Time	Received by	Date	Time
	Relinquished by	Date	Time	Received by	Date	Time
	Relinquished by	Date	Time	Received by	Date	Time

Instructions for Use of the Request/Chain of Custody Form

Basis of Request:	Incidents of civil/criminal nature, traffic accident, etc.
Requested Format:	State whether data is required on a Digital Video Disk (DVD), Compact Disk (CD), or other format required for storage. Data will be saved to the media in the format requested (i.e. *.avi or *.wmv). In very limited cases, a hard drive may be removed if approved by MIS Deputy Chief Love or designee and Security .
Indicate Bus No:	Provide Bus Number.
Point of Contact:	DDOT POC, include the requestor's name.
POC Phone No:	DDOT POC phone number.
Scope & Comments:	Provide type, location, description including date with start and stop times for recording and any additional information, instructions, comments for the request submitted. Remember there are limitations to the storage media.
Relinquished By:	The one to relinquish the content signs dates and indicates the time of content transfer.
Received By:	The receiver of the content signs dates and indicates the time of content receipt.

Request/Chain of Custody Details

Process

These documents will be completed for every internal/external data request. See the Data Request Procedure below for additional information on that process.

Retention

Mobile data is generally available for 28 days. **MIS Operations Manager, Transit Police and Security** will be the departments responsible for the retention, storage and administration of these documents as they are requested.

Best practice dictates that the requesting party within DDOT should also maintain a copy.

Data Retrieval Authority Procedure

Purpose

This document is intended to clarify who will have access to the VVS content, as well as the process of accessing this data. The reason for making these procedures unequivocal is due to the nature of video content.

Data Availability

Mobile data is generally available for 28 days. Downloads from the revenue fleet to the network are triggered based on incidents described in the "Data Retrieval Process" below. Network data is stored in accordance with DDOT MIS rules.

Scope

This document spells out who can access VVS content, and it also covers the procedures of retrieving VVS content.

Definitions

VVS content will be defined as video footage from a DDOT vehicle.

VVS data will be defined as VVS content included with the VVS systems data, which includes: the data, location, and equipment of capture.

"Of Interest" content is VVS data that has been deemed necessary to retain.

Tagging is the process of adding additional information to an electronic record/file via the use of data.

Procedures

Data Retrieval Authorization by specified members of **MIS** are authorized and trained to retrieve VVS system content directly from the DVR or wireless access systems. Wireless signal is protected from unauthorized access by encryption. Presently, viewing of content is limited to one fixed wireless access point located in Building F at Shoemaker Garage. Anyone outside of **MIS** should not have access to the content without their supervision.

Mobile or remote viewing of content is currently not possible since cellular links, city wide wireless points, or mobile wireless antennae are not available.

Responsibilities

MIS will be responsible for ensuring that logical access controls are in place so that only authorized individuals may access VVS content.

MIS and Director or designee are responsible for ensuring that physical access controls are in place so that only authorized individuals may access VVS content. Although the **Director** will likely assign a designee to the task of monitoring access controls, the **Director** will have primary responsibility that the maintenance of the VVS system including the DVR is being conducted. **Deputy Chief Love will coordinate with Paul Jameson to update protocols for physical access controls.**

Data Retrieval Process

Civil Incident Downloads

The Driver calls Dispatch with an incident and/or it is reported on the daily Drivers' Incident/Accident Report. Once received at Dispatch, Drivers Supervisor completes a Request/Request/Chain of Custody Form and forwards the request to VVS Administrator. **MIS** staff then downloads the content wirelessly when the vehicle is at the garage. **MIS** then burns a DVD, and the **Director or Director's Designee (Deputy Chief Love)** then picks up the DVD from the **VVS Administrator** at 1301 East Warren Avenue.

Criminal Incident Downloads

The Driver calls Dispatch with an incident. If it is criminal in nature **Transit Police** responds. **Deputy Chief Love or designee completes a Request/Chain of Custody Form.** The hard drive may be sequestered or a request made for the DVR video to be downloaded from the vehicle at the scene. **Deputy Chief Love or designee will be responsible for following the above procedures for extracting a hard drive or viewing video by the Detroit Police Department.** If the video is admissible as evidence **MIS will burn a DVD** of the content, and put in a request for **MIS** to tag the content as 'of interest' and to make a copy for the **Prosecutors Office.** **Any release of video will follow the above procedures outlining video or hard drive dissemination.**

Data Drive Pull Incident Response

Transit Police or MIS team will complete a Request/Chain of Custody Form and then pull **the DVR hard drive and the vehicle in question is pulled offline.** This event is triggered/tracked by **VM Supervisor.** **VM** staff will install a replacement drive. **VM Supervisor** then notes the vehicle/DVR drive is operable and returns it to service.

Union Matters

Director or designee completes a Request/Chain of Custody Form and forwards it to **MIS,** which ensures the system downloads the DVR video from the vehicle and burns the content to a DVD. The requestor then picks up the DVD from the **VVS Administrator** at 1301 East Warren Avenue.

Data Request Handling Procedure

Purpose

This document defines the procedures for DDOT employees, third-parties and affiliates to follow for requesting VVS video content. This procedure exists as inappropriate use exposes DDOT to risks including the compromise of personal privacy, and legal issues.

Scope

This document covers the procedures for granting access to VVS data for internal and external customers.

Definitions

VVS content will be defined as video footage from a DDOT vehicle.

VVS data will be defined as VVS content included with the VVS systems' data, which includes: the data, location, and equipment of capture.

As defined within the context of this procedure, "internal" customers refer to DDOT employees or contract staff.

DDOT has defined "external" customers as entities that are not DDOT W-2 employees, or directly affiliated with DDOT, who may have an interest in accessing VVS data/content. Third parties and external customers will be used interchangeably/synonymously in this document.

Responsibilities

MIS will be responsible for burning DVD's and/or installing the viewing software for access to VVS content. **MIS** will also be responsible for ensuring that all DDOT parties have completed the Request/Chain of Custody Form prior to providing this content.

Transit Police or Security will be responsible for approving and retaining the Request/Chain of Custody Forms and acceptable use policies for this process.

When an external party is involved, **MIS** in coordination with the **City of Detroit Legal Department**, **Transit Police** may also provide review of the Request/Chain of Custody provided.

Procedures

Interested internal parties will complete The Request/Chain of Custody Form and then forward it to the **VVS Administrator**. External parties will interface with **City of Detroit Legal Department or Transit Police** who will complete a Request/Chain of Custody Form and then forward the request to the **VVS Administrator**.

The **VVS Administrator** will document the request in the VVS Request Log, and prioritize the request based upon its urgency. **MIS** will receive the Request/Chain of Custody Form.

Sever is configured for download by **MIS**.

Vehicle is located and sequestered for wireless transfer of data to server.

MIS downloads the specified VVS content, burns the content onto a DVD, labels the DVD, electronically populates the **MIS** portion of the Request/Chain of Custody Form, prints it out and signs it.

This Request/Chain of Custody system and the VVS Request Log will memorialize creation DVD for tracking and auditing.

DDOT will create separate procedures to use in the event VVS content needs to be restored due to data corruption.

The **VVS Administrator** notifies the DDOT party who requested the content (directly or on behalf of an external party), and asks that they pick up the DVD.

The DDOT party signs the Request/Chain of Custody Form from **MIS**, receives a copy of it, and picks up the DVD.

If an external party is to receive the DVD next the DDOT function (**MIS** in coordination with the **City of Detroit Legal Department, Security, or Transit Police**) responsible completes the approval section of the Request/Chain of Custody Form, and has the external party sign it.

Data Retention and Destruction Procedure

Purpose

This document is intended to help employees determine what VVS content to retain, and how long to retain it, and how to destroy it. Any employees with questions regarding this procedure should go see their supervisor.

Scope

This document covers the procedures for retaining and destroying VVS content.

Definitions

VVS content will be defined as video footage from a DDOT vehicle. VVS data will be defined as VVS content included with the VVS systems' data, which includes: the data, location, and equipment of capture.

Responsibilities

MIS will be responsible for the physical and logical storage of the VVS content, as well as to ensure that the content is properly backed-up. Additionally, MIS will coordinate the destruction of VVS content and hardware as deemed necessary. MIS and the Directors Designee will be responsible for re-evaluating this procedure on an annual basis.

Procedures

Record Retention

General Video Content

All content will be retained pertaining to the capacity of hardware and systems involved during normal business practices. Hardware includes DVR devices, local servers, and centralized storage. In the event of an incident, video will be copied to a DVD (Digital Video Disc) and retained as part of the incident file.

On-Board Revenue Fleet Video Content

All content is stored 28 days.

Criminal Investigation Content

If a request was made for storage of data, best practices indicate criminal investigation content be retained on centralized storage for five (5) years, with the understanding that Transit Police will retain a DVD copy in their case files.

Civil Investigation Content

If a request was made for storage of data, Best practices indicate civil investigation content should be retained on centralized storage for three (3) years, with the understanding that DDOT Claims will retain a DVD copy in their case files.

Accident Content

If a request was made for storage of data, all content is stored in accordance with Civil Investigations above.

Record Destruction

Mobile View DVRs & Data Drives

All VVS data drives will over-write previous content from prior recordings; however, when the drives reach end-of-life status **MIS** will ensure that all data is removed by secure overwriting, degaussing or shredding internally, by a separate party or by the VVS system vendor.

Storage Data Drives

The centralized VVS system storage facility at 1301 East Warren Avenue St. will be configured to over-write legacy content (any content 112 days or older); however, when the storage drives reach end-of-life status **MIS** will ensure that all data is removed by secure overwriting, degaussing or shredding internally, or by a separate party.

DVDs

To ensure that VVS DVD content is secured when it reaches end-of-life status DDOT will place shredders at the 1301 East Warren Avenue facility, and instruct employees to use these shredders for legacy VVS DVDs.

Vehicle Video Maintenance Responsibilities and Procedures

Purpose

This document is intended to identify the responsibilities and maintenance for the installation, troubleshooting, and support of the VVS for assigned Buses. This includes all hardware, software and network infrastructure in use for the VVS by DDOT.

Scope

This document covers the responsibilities and procedures of the VVS and infrastructure.

Definitions

VVS Content will be defined as video footage from a DDOT vehicle.

VVS Data will be defined as VVS content included with the VVS systems' Data, which includes: the data, location, and equipment of capture.

VVS Hardware is defined as the cameras, DVR, associated antennas, Local Area Network (LAN) Servers, wired and wireless infrastructure and any other hardware specifically designated for the VVS.

VVS Software includes all software associated with the VVS. This includes operating systems residing on the DVR which is an embedded version of Microsoft Windows operating system (OS), DDOT personal computer (PC) assigned to the task of Server with OS currently defined as Microsoft Windows Server, and proprietary software associated with the VVS vendor. Unauthorized access during wireless transmission is limited by encryption.

VVS Configuration Settings include the accepted hardware and software configurations of all associated hardware and software related to the VVS. Configuration settings are initiated and set up by VVS vendor for the continued use of the VVS.

Responsibilities

MIS will be responsible for the installation, maintenance, and troubleshooting for the network architecture and infrastructure related to the VVS. This includes all wired network connectivity, wireless network connectivity using wireless infrastructure, LAN servers at all remote locations and data integrity with respect to data captured on DVRs. In addition, **MIS** will provide the second level support to **Vehicle Maintenance (VM)** personnel and **Quality Assurance and Research (QAR)** staff with respect to troubleshooting issues on revenue vehicles related to VVS. This includes cameras, connectivity, and DVRs.

QAR Division Staff will be responsible for supporting **MIS** with the fleet wide physical operation of onboard equipment and interaction of that equipment with the network. **QAR** staff will also work with VVS Vendor and engineering staff to assess health of the revenue fleet.

Vehicle Maintenance (VM) staff will be responsible for the daily check out of camera and DVR operations on each revenue vehicle. This may consist of connecting directly into DVRs on revenue vehicles with a laptop to verify successful camera operations and recording to DVRs prior to the revenue vehicles beginning operations. **VM** will also be responsible for troubleshooting and replacing cameras and/or DVRs deemed defective during the checkout process or after operation of the revenue vehicle.

VM Personnel will utilize the DDOT Help Desk Service in cases where problem resolution cannot be determined by **VM** staff or additional equipment is needed to replace hardware on revenue vehicles.

The VVS Vendor and engineering staff, with the guidance of **QAR**, **MIS**, and **VM** personnel, will be responsible for new installations and retrofit configurations of the VVS on assigned revenue vehicles and supporting facilities.

Procedures

Revenue Vehicle Maintenance

Maintenance and 1st level troubleshooting of the VVS on revenue vehicles including cameras, cabling, and DVR operations will be performed by **VM** staff. **MIS** will assist, support and provide troubleshooting on any issues that cannot be resolved by 1st level support. First level support includes connecting directly to the DVR with a laptop computer to verify camera and cabling operations and initial troubleshooting of DVR devices including the replacement of hard drive caddies if determined source of failure.

DVR and Hard Drive Maintenance

DVR and hard drive maintenance will be the responsibility of **VM**, **QAR**, and **MIS** staff in the event of failure of either device. **VM** will test and run diagnostics on DVR devices to verify operation including removal and replacement of the hard drive caddy. In the event of a hard drive caddy replacement, proper Request/Chain of Custody forms will be completed and the hard drive caddy will be returned to the **MIS** department for further troubleshooting or replacement.

LAN Server & Network Connectivity Maintenance

All LAN Server and network connectivity will be the responsibility of the **MIS** department. This includes troubleshooting and testing of wireless connectivity from the revenue vehicles to the local LAN server and wired network connectivity from the LAN server to DDOT headquarters. **VM** staff will contact the DDOT helpdesk in cases where LAN connectivity (wired or wireless) is not available and if access to the local LAN server is unavailable.

STAFF

The procedures within this document require coordination between Detroit Department of Transportation (DDOT) staff and contract staff to administer these procedures. Titles and present staffing is listed below.

Staff Title	Department	Staff Name
District Attorney		
Director	DDOT	Dan Dirks
Director's Designee	Transit Police	Deputy Chief Dwayne Love
City of Detroit Legal (1)		
City of Detroit Legal (2)		
DDOT Security Administrator		
DDOT Security Staff		
Transit Police (1)	Transit Police	Chief Sidney Bogan
Transit Police (2)	Transit Police	Sergeant Kristy Cross
Transit Police (3)	Transit Police	Sergeant Derrick Russ
VVS Administrator (1)		
VVS Administrator (2)		
MIS (1)		
MIS (2)		
QAR (1)		
QAR (2)		
QAR (3)		
Driver		
Driver Supervisor (1)		
Driver Supervisor (2)		
Driver Supervisor (3)		
Driver Supervisor (4)		
Driver Supervisor (5)		
Driver Supervisor (6)		
Driver Supervisor (7)		
VM Staff		
VM Supervisor (1)		
VM Supervisor (2)		
VM Supervisor (3)		

MASTER AGREEMENT

BETWEEN THE

CITY OF DETROIT

DEPARTMENT OF TRANSPORTATION

AND

AMALGAMATED TRANSIT UNION, AFL-CIO - LOCAL 26

2014 – 2018

to the Union, and offer to meet and confer with the Union for a period not longer than thirty (30) days in order to discuss potential modifications to the terms of the Medical Plans or to the allocation of contributions to the cost of medical coverage by the City and the Employees in order to comply with the requirements of PA 152. To the extent the City and the Union are unable to reach an agreement within thirty (30) days, the City may make any necessary modifications to ensure compliance with PA 152.

41. EMPLOYEES SERVING ON JURY DUTY

- A. An Employee who serves on jury duty will be paid the difference between his/her pay for jury duty and his/her regular day's pay for all days he/she is required to serve on jury duty.
- B. In the event that an Employee reports for jury duty but is not selected to actually serve on a jury, he/she will be paid the difference between the jury pay received and his/her regular day's pay and be excused for the day, exclusive of travel pay.
- C. In order to receive payment for jury duty, an Employee must have been regularly scheduled to work on a non-overtime basis and, within ten (10) days of completion of serving on jury duty, he/she must turn in documentation received from court to the departmental supervisor of such service, otherwise, all monies paid will be recovered by the Department.
- D. Run holders will be paid for the difference between pay for jury duty and pay for their regularly scheduled runs. Extra persons will be paid the difference between pay for jury duty and eight (8) hours.
- E. An Operator serving on jury duty shall report for scheduled work on any day he/she is not required to serve on jury duty.
- F. An operator who is required to serve on jury duty is not required to report for work that day regardless of the time of their scheduled work.

42. MISCELLANEOUS

- A. Active and retired Employees will be permitted to ride without charge upon presentation of a current pass card or a retirement pass card.
- B. Within seven (7) days of its effective date, the City shall provide the Union with an electronic copy of the Agreement.
- C. The City may offer Operators an employee loan program, the terms of which may be changed from time to time at the discretion of the City.
- D. Use of Surveillance Equipment and GPS Equipment.
 - 1. The City of Detroit has established the use of surveillance equipment and GPS equipment to provide a safe and secure environment for passengers and Employees.
 - 2. Information from surveillance equipment and GPS equipment may also be used to train and counsel operators. In addition, such information may be used to

investigate potential misconduct and to support disciplinary measures in cases in which the Department has received a complaint or otherwise has a reasonable basis for believing that misconduct has occurred.

3. In gathering video evidence from surveillance equipment for use in disciplinary matters, the Department may consider any video from between ten (10) minutes before and ten (10) minutes after the incident at issue. This limitation shall not apply in any case involving alleged criminal acts (including, but not limited to assault, robbery, theft, or driving offenses) or in any case involving an alleged threat to public safety.
4. The Union has the right to review all video and audio used as evidence in disciplinary actions.

43. UNIFORMS

- A. The Department shall have the right to require Employees to wear uniforms in accordance with policies established by the Department. Any Employee not wearing a clean uniform, or wearing items not a part of the designated uniform, will be considered "OUT OF UNIFORM".
- B. Initial Issue. At time of hire, the Department shall provide all new Operators with an initial uniform. In the alternative, the Department may institute a uniform voucher system and issue Employees uniform vouchers in lieu of an initial uniform. Operators shall be ineligible to receive an annual uniform allowance in accordance with Section C until he or she has completed two (2) years of service.
- C. Annual Uniform/Cleaning Allowance. Employees having completed two (2)* years of service and who are actively working in the classification of T.E.O., shall be granted an annual uniform/cleaning allowance totaling five hundred dollars (\$500) to be paid in the amount of two hundred and fifty dollars (\$250) twice yearly. These payments shall be made in the months of September and April. Employees shall be responsible for procuring uniforms according to Department specifications. Operators who, for any reason, are not actively working in the capacity of T.E.O. during the week the uniform/cleaning allowance is issued will not be entitled to receive a uniform allowance at that time. However, upon his/her return to work and after actively working a full regularly scheduled work week, the Operator will be issued a uniform allowance at that time.

*Each year of service is twelve (12) months of eighteen (18) paid days.

- D. T.E.O.'s uniform will be composed of the following clothing items:

Garrison Hat, Shirt, Trousers/skirt, Tie, Eisenhower Jacket, Winter Jacket (Also, customary ancillary uniform items, such as turtleneck, polo summer shirt, belt, shorts, sweater, baseball cap, and skull cap will be allowed to be worn in the appropriate, authorized color and must adhere to D-DOT's regulations).

City of Eau Claire Transit, Eau Claire, Wisconsin

City of Eau Claire Owned and Operated Cameras Policy, January 10, 2014

12



Department of Human Resources

CITY OF EAU CLAIRE OWNED AND OPERATED CAMERAS POLICY

January 10, 2014

PURPOSE AND SCOPE

The City of Eau Claire operates a system of cameras for the purpose of creating a safer environment for all those who live, work and visit the City. This policy explains the purpose of the cameras and provides guidelines for their operation and for the storage of captured images.

POLICY STATEMENT

Cameras may be placed in strategic locations throughout the City or in certain vehicles or equipment. These cameras can be used for detecting and deterring crime, to safeguard against potential threats to the public, to manage emergency response situations during natural and man-made disasters, and to monitor the use of publicly owned buildings, facilities, vehicles, equipment and operations, as well as to assist City officials in providing quality services to the community. Cameras placed for the primary purpose of monitoring City owned buildings, facilities, vehicles, equipment or operations must be approved by the appropriate Department Director. Cameras placed in public spaces for the primary purpose of monitoring public activity must be approved by the Chief of Police.

MONITORING

Images from fixed cameras will be recorded on a 24-hour basis every day of the week. Images from cameras in vehicles or equipment will be recorded during operation of the vehicle or equipment. Only authorized and trained employees are allowed to access these images. When activity warranting further investigation or review is reported or detected at any camera location, the employee may selectively view the appropriate camera and relay any available information to responding units or other employees as necessary to appropriately respond to the situation. The employee operating the cameras is authorized to adjust the cameras to more effectively view a particular area for any legitimate public purpose.

Recorded images may be used for a variety of purposes, including to:

- (a) Assist in criminal investigations.
- (b) Monitor activity around high-value or high-threat areas.
- (c) Assist in identifying, apprehending and prosecuting offenders.
- (d) Assist in gathering evidence for criminal and civil court actions.
- (e) Help emergency services personnel maintain public order.
- (f) Monitor pedestrian and vehicle traffic activity.
- (g) Help improve the general environment on the public streets.
- (h) Assist in providing effective public services.
- (i) Assist in the management of natural or man-made disasters.

TRAINING

Personnel involved in video monitoring and operations must be appropriately trained prior to being provided access to the camera system.

PROHIBITED ACTIVITY

Video monitoring will be conducted in a professional, ethical and legal manner at all times. The safety system will not be used to invade the privacy of individuals or look into private areas or areas where the reasonable expectation of privacy exists. All reasonable efforts will be taken to protect these rights. Video monitoring shall not be used to harass, intimidate or discriminate against any individual or group.

MEDIA STORAGE

All video media will be stored in a secure area with access restricted to authorized persons. Cameras operate on a continuous loop. The timing for recorded loops will be set according to the specification of the equipment. Any recordings needed as evidence in a criminal or civil proceeding shall be copied to a suitable medium and booked into evidence in accordance with current evidence procedures. Any recordings that are captured, saved or retained from the continuous loop should be treated as a record subject to the open records laws.

REVIEW OR RELEASE OF VIDEO IMAGES

Recorded videos are classified as public records (Wis. Stat. § 19.32(2)). As such, all requests for the release of video records must be processed as open records requests and follow the appropriate procedures. The open records request review process is as follows:

Video images collected or retained for Police Department purposes: The review or release of video images collected or maintained by the Police Department shall be done only with the authorization of the Chief of Police or an authorized designee.

All other video images collected or retained by the City of Eau Claire: Requests to review or release video images collected or maintained by the City of Eau Claire (other than the Police Department) shall be done only with the authorization of the Director of Human Resources or an authorized designee.

AUTHORIZATION AND TRACKING OF THE PUBLIC AREA CAMERA SYSTEM

Authorization for access to public area cameras must be approved by the Department Director.

The City of Eau Claire's Information Services Manager will be responsible for maintaining:

- (a) A list of all employees authorized to access the camera system.
- (b) A record of the location of all active cameras in the system.
- (c) All video files per the records retention policy on file with the State of Wisconsin.

City of Gardena Municipal Bus Lines (GTrans), Gardena, California

City of Gardena, Resolution No. 6235, Establishing a Retention Policy for
GTrans Video Surveillance Recordings

13



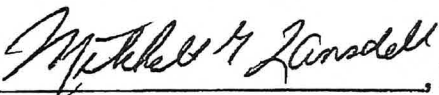
City of Gardena
City Council Meeting

AGENDA REPORT SUMMARY

Agenda Item No. 8. A. (1)
Department: ELECTED and
ADMINISTRATIVE
OFFICES
Meeting Date: 07/12/2016
Resolution No. 6235

TO: THE HONORABLE MEMBERS OF CITY COUNCIL

**AGENDA TITLE: RESOLUTION NO. 6235, ESTABLISHING A RETENTION POLICY FOR
GTRANS VIDEO SURVEILLANCE RECORDINGS**

COUNCIL ACTION REQUIRED: Adopt Resolution No. 6235	<u>Action Taken</u>
RECOMMENDATION AND STAFF SUMMARY: Staff respectfully recommends that the City Council adopt Resolution No. 6235, which establishes a retention policy for GTrans video surveillance recordings. Approximately one (1) year ago, GTrans installed and deployed Apollo Video Technology cameras and storage equipment on all GTrans buses. The installation was done to support the safety and security of employees and the riding public, as well as to preserve records of reported incidents. California Government Code Section 34090.8 requires that installed systems shall be capable of storing images for at least one (1) year, unless: <ol style="list-style-type: none">(1) The transit agency has made a diligent effort to identify a security system that is capable of storing recorded data for one (1) year.(2) The transit agency determines that the technology to store recorded data in an economically and technologically feasible manner for one (1) year is not available.(3) The transit agency purchases and installs the best available technology with respect to storage capacity that is both economically and technologically feasible at that time; an The City Council determined that the Apollo system, at the time it was purchased, was the best available technology with respect to economic and technological storage capacity and that, while storage capacity of all recorded data is not feasible with the system, it does allow for retention meeting the requirements of Government Code Section 34090.8 with respect to any incident or claim reported prior to the video data being overwritten which, in normal circumstances, will be not less than thirty (30) days. Adoption of Resolution No. 6235 meets the retention policy requirement of California Government Code Section 34090.8. Staff did meet with the Gardena Municipal Employee Association Board of Directors and reviewed the proposed policy, contained in Resolution No. 6235, with them.	
FINANCIAL IMPACT/COST: None	
ATTACHMENT: Resolution No. 6235	
Submitted by <u></u> , Mitchell G. Lansdell, City Manager Dated: 07/07/2016	

RESOLUTION NO. 6235

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF GARDENA, CALIFORNIA, ESTABLISHING A RETENTION POLICY FOR GTRANS VIDEO SURVEILLANCE RECORDINGS

WHEREAS, the City of Gardena, after a diligent effort to secure a video system that is capable of storing data economically for the longest feasible time, installed Apollo Video Technology cameras and storage equipment on all GTrans buses in order to support the safety and security of its employees and the riding public, and to preserve records of reported incidents; and

WHEREAS, California Government Code Section 34090.8 provides that installed systems shall be capable of storing images for at least one year, unless:

- (1) The transit agency has made a diligent effort to identify a security system that is capable of storing recorded data for one (1) year.
- (2) The transit agency determines that the technology to store recorded data in an economically and technologically feasible manner for one (1) year is not available.
- (3) The transit agency purchases and installs the best available technology with respect to storage capacity that is both economically and technologically feasible at that time; and

WHEREAS, the City Council has determined that the Apollo system, at the time it was purchased, was the best available technology with respect to economic and technological storage capacity and that, while storage capacity of all recorded data is not feasible with the system, it does allow for retention meeting the requirements of Government Code Section 34090.8 with respect to any incident or claim reported prior to the video data being overwritten which, in normal circumstances, will be not less than thirty (30) days.

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF GARDENA, CALIFORNIA, DOES HEREBY FIND, DETERMINE, AND RESOLVE, AS FOLLOWS:

SECTION 1. GTrans may generate surveillance video through the use of electronic devices located on buses or in places which are open to the public, and may use the video for business purposes. No person has any expectation of privacy while located in "public places" that include all GTrans Transportation Facilities, and vehicles. The locations where GTrans operates buses, and boards and alights transit customers that are generally within the public right-of-way are areas open to the public and are, thus, "public places." Persons using GTrans Transportation Facilities, and who are in or on public conveyances and/or in such "public places" have no expectation of privacy. GTrans may use video surveillance in such places without qualification or restriction, and may utilize the images thereby obtained in whatever way best meets the needs and objectives of GTrans.

SECTION 2. Surveillance video recordings will be stored on a hard drive that is maintained as a part of the recording system with the bus cameras / bus. The data will be maintained on the hard drive until the video footage is overwritten. Unless a specific need for the data is raised within the period of normal retention, the data will ordinarily be overwritten and lost. Video footage, for which a business need is identified within the period of retention, shall be reproduced and otherwise retained at a different location, as follows:

(1) Video recordings or other recordings that are evidence in any claim filed or any pending litigation shall be preserved until the claim or the pending litigation is resolved plus one (1) year.

(2) Video recordings or other recordings that record an event that was or is the subject of an incident/accident report or was automatically downloaded shall be reviewed and, if no relevant data is contained thereon, may be overwritten or erased within fourteen (14) days thereafter.

(3) Video recordings or other recordings that record an event that was or is the subject of an incident/accident report or was automatically downloaded shall be reviewed and, if they contain relevant data, they shall be retained until the incident is resolved and, in any event, for not less than one (1) year.

SECTION 3. The retention policies set forth herein fully meet the retention requirements of Government Code Section 34090.8.

SECTION 4. That this Resolution shall be effective immediately.

BE IT FURTHER RESOLVED that the City Clerk shall certify to the passage and adoption of this Resolution; shall cause the same to be entered among the original Resolutions of said City; and shall make a minute of the passage and adoption thereof in the records of the proceedings of the City Council of said City in the minutes of the meeting at which the same is passed and adopted.


Passed, approved, and adopted this _____ day of _____, 2016.

MARK E. HENDERSON, Mayor Pro Tem

ATTEST:

MINA SEMENZA, City Clerk

APPROVED AS TO FORM:



PETER L. WALLIN, City Attorney

FOR YOUR SAFETY
THIS VEHICLE MAY BE EQUIPPED
WITH A
VIDEO AND AUDIO
OBSERVATION SYSTEM.

© 2012 RideGTrans, Inc. All rights reserved.
This vehicle is equipped with a video and audio observation system.
For more information, please contact RideGTrans, Inc.



**FOLLOW
GTRANS ON
SOCIAL MEDIA
@RideGTrans**



GTRANS

Website: www.ridegtrans.com

© 2012 RideGTrans, Inc. All rights reserved.

760

Unauthorized Conspicuous
Use of Green is
Prohibited by Law

EMERGENCY
EXIT

Dallas Area Rapid Transit (DART), Dallas, Texas

DART Police Special Order, Procedures on Release and Handling of
DART Video

15

DART POLICE SPECIAL ORDER



No. _____

To: DART Police Personnel

Date: TBD

Subject: Procedures on Release and Handling of DART Video

I. PURPOSE

The purpose of this order is to establish guidelines for the handling and release of all DART video. All policies outlined in General Order 04-05, Handling and submission of evidence and property will apply.

II. POLICY

The objective of this order is to ensure that all DART Police personnel comply with DART policies and procedures when handling and releasing video.

- A. No member of the DART Police Department shall release any DART video camera footage to any person. Exceptions to this rule are:
 - a. Chief of DART Police or his designated representative
 - b. Lawful subpoena
 - c. Open Records Request
 - d. Agency with a Criminal Justice Function
- B. At no time will any person or department retain or duplicate any video without the written approval of the Chief of Police or his designee.
- C. All internal and open records requests for release of video will be referred to the Records Management Supervisor (RMS).
- D. All Law Enforcement agencies and district attorney officer's requests for release of video will be referred to the Criminal Investigations Department (CID).
- E. Shift Investigators and Camera Monitors may retrieve initial video immediately after an incident has occurred to provide to the Crime Scene Supervisor or his designee video to assist in identification of suspect(s) or assessment of the incident.
- F. Crime Scene Video will be retrieved by the Video Systems Administrator or designated personnel within 48 hours after a legal request has been made. This video will provide all views recorded covering the crime scene area.
- G. ALL video retrieved must be logged before distribution and signed for by the receiving officer.
- H. No video will be created in .AVI or .WMA format unless instructed by the Video Systems Administrator or DART Chief of Police.

III. DEFINITIONS

- A. "DART's Legal Department" refers to the person(s) in the DART Legal Department responsible for releasing information to the requestor through the Public Information Act.
- B. "Open Records Request" is a written request for documents submitted by a person pursuant to the Public Information Act.
- C. "Non-Open Records Request" is a request for video that is released to internal DART personnel only. Video released internally may not include any video involving an investigation or video that may include any criminal act.
- D. "Video Systems Administrator (VSA)" refers to the individual(s) responsible for the overall management of the video camera systems.
- E. "Shift Investigator" refers to officer(s) that are trained as Shift Investigators and are responsible for downloading video and maintaining the chain of custody until it is processed into evidence.
- F. "Initial Video" is defined as video that may be retrieved immediately after an incident has occurred, by Camera Monitors, Shift Investigators or CID, which would assist officers in the identification of suspects and assessment of the crime scene.
- G. "Crime Scene Video" is video provided by the Video Systems Administrator or designated personnel, from all cameras which cover the crime scene area, to be retrieved 48 hours after a legal request has been made.
- H. "Retain or Duplicate" is defined as computer media (eg., flash drives, CD's, DVD's, computers or local network drives) that have not been designated as DART Police evidence storage.

IV. REQUESTING PROCEDURES

- A. Request for video will be processed only after the following requirements are met:
 - 1. **Internal Request:** - only processed after receiving a departmental work flow. The work flow must provide: dates, times (as close to the incident as possible), location of the incident, a brief description of what the video should provide, and a related service number, if applicable.
 - 2. **Open Records Request-** Will be processed after review by Legal and sent to the Records Management Supervisor. Video that is released to the Attorney General will be converted to a Windows Media file. All other requests will be in a proprietary format. The video will be released to DART Legal through the Records Management Supervisor or designee.
 - 3. **Internal Affairs-** Will only be processed after receiving a departmental workflow. The work flow must provide: dates, times (as close to the incident as possible), location of the incident, a brief description of what the video should provide, and a related service number, if applicable.

4. **Tracking employee actions** - DART will NOT provide video for tracking the daily activities of employees for policy compliance UNLESS the activity is of a criminal nature.
5. **Officer Request**- The VSA will only process a request after receiving a departmental workflow that is approved through the officers' chain of command. The work flow must provide: dates, times (as close to the incident as possible), location of the incident, a brief description of what the video should provide, and a related service number, if applicable.
6. **Special Request/Viewing** – Requests that do not meet any of the above listed criteria will be required to provide: dates, times (as close to the incident as possible), location of the incident, a brief description of what the video should provide, and a related service number, if applicable. This video will be approved by the Video Systems Administrator or the DART Chief of Police.

V. PROCEDURES

- A. Processing requests for DART Police video by Police Dispatch – upon receiving a request for police video, the camera monitor should respond as follows:
 1. Through verbal (followed up by a workflow) or Workflow request, make sure a general description, location and time as to when the incident occurred is provided.
 2. Camera Monitors will choose the camera that best reflects the incident and provide footage of the requested incident including one minute prior to and one minute after the incident occurred.
 3. In addition, Camera Monitors may provide snapshots or photos that will assist in identification of any and all suspects.
 4. Camera Monitors will log the date, start time, end time, camera number and station location. Monitors will also log their name, the requesting officer's name, disk number and obtain the signature of the officer receiving the video.
 5. Camera Monitors will provide video for initial video requests only, unless directed by the VSA or RMS.
- B. Processing requests for Open Records Requests – upon receiving the request for police video, the Public Safety Technology (PST) or Records Management Supervisor(RMS) should respond as follows:
 1. Through Workflow or Open Records Request, make sure enough information is provided to locate the video.
 2. The PST or RMS will determine which camera best reflects the incident and provide footage of the incident according to the times requested in the open records request. If no times were specified in the request, footage of the incident will be provided to include one minute prior to and one minute after the incident.
 3. The PST will log the date, start time, end time, camera number and station location. The PST or PST will also log the requestor's information and provide a copy of the request in the log book.
- C. Public Safety Technology(PST) will in the event of a major incident, provide video within 24-48 hours after a legal request has been made:

1. Using the log times from the camera monitors of an incident, the Video Systems Administrator will provide video of all cameras covering the crime scene area.
2. Video will be created in two formats, Windows Media (WMA) and Video Management Software (VSOM) format CVA. The Video Systems Administrator will also provide instructions on the disk of video formats and operating procedures for viewing the video.
3. The Video Systems Administrator will ensure that once the video is created, it is secured as evidence.

D. Verbal request of video by Officers/Supervisors:

1. Request Video verbally (with a follow up workflow) or through work flow; provide description, location and time as to when the incident occurred.
2. Ensure that requesting officer provides name and signature upon receiving the video. Upon receiving video the Officers/Supervisors must log the video into evidence.

E. Releasing to other Law Enforcement agencies by CID – upon receiving a request for video, CID should respond as follows:

1. CID will log the date, start time, end time, camera number and station location. CID will also log the agency name, the requesting officer's information, disk number and obtain the signature of the officer receiving the video.
2. Ensure that the requesting officer provides name and signature upon receiving the video.

F. Shift Investigators, upon request to download video for criminal investigation and/or internal purposes (as requested through IA or a Lt. or Sgt.) will:

1. Ensure a detailed description, location and time of the incident is provided.
2. Determine which camera best reflects the incident and provide footage of one minute prior to and one minute following the incident,
3. Log the date, start time, end time, camera number and station location. The Shift Investigator will log the requestor's information and provide a copy of the request in the log book.
4. Follow policy as outlined in General Order 04-05 Section V C.

G. Video footage of Juveniles

1. Video footage of juveniles will only be released to another criminal justice agency, according to court order or as determined through the Public Information Act open records process.

VI. Retention

- A. All departments subject to the release of video will maintain a video log as outlined in appendix A of this document. In addition to the log information, departments will complete a Video request Chain of Custody Form as outlined in appendix B.
- B. Both appendix A and appendix B will be maintained for at least one year from the latest date of release, logged.

VII. Forms and Documents

- 1. Appendix A - Example of a Log File
- 2. Appendix B - Example of a Video Request Chain of Custody Form

I approve of this document as DART Police policy and procedure for the release and handling of all DART video, and appoint the Public Safety Technology Manger/VSA as the point of contact for all document updates and changes.

James D. Spiller
Chief of Police

Distribution List:

Deputy Chief
Bureau Capt's

CID
Internal Affairs
Police Dispatch
Mangers
Record Supervisor

[illegible]



DART Police department

VIDEO REQUEST CHAIN OF CUSTODY FORM



On _____ (Date) I _____ (Title Name and Badge# or ID#)

Verified chain of command approval through from DART online service request

Workflow # _____ for video of: _____

Facility/Vehicle/Location: _____

Date: _____ Requested by: _____

Agency /Incident #: _____

Offense #: _____ Media Type: _____

Footage Released Notes: _____

Archive Saved By _____ Date _____

Disc Downloaded By _____ Date _____

Released By _____ Date _____

Released To _____ Date _____

Number of Disk Released: _____

FOR LAW ENFORCEMENT USE ONLY



OPERATIONS POLICY/PROCEDURE

OFFICE OF PRIMARY RESPONSIBILITY: DART Police		EFFECTIVE DATE: TBD	No:
SUBJECT: Surveillance Video Requests		AUTHORIZATION: Operation Chief	DATE:
PAGE 1 OF 3 PAGES			
New (X) Amends () Rescinds () Replaces ()			

OBJECTIVE:

This Operations Order provides guidelines for when video surveillance recordings can be requested and who is authorized to make the request. This Order applies to all video surveillance systems that are controlled by DART Police. Surveillance video requested under this Order must be for DART official business. All personal requests will go through the Legal Department consistent with other requests for information.

SCOPE:

Applies to all DART employees and contractors.

DEFINITIONS:

Fixed Surveillance: Surveillance systems at passenger facilities and DART operational and administrative buildings

Mobile Surveillance: Surveillance systems on buses, light rail vehicles and mobile towers.

1. DART Police video surveillance is responsible for the safety of DART property and passenger security.
2. Transportation Department Drive Cam Video system will provide information on the Drivers and Vehicle operational performance of the DART bus. This video is not controlled by DART Police.

CONCEPT OF OPERATIONS:

The fixed facility surveillance cameras consists of fixed cameras covering the boarding areas, TVM's, PEC's, designated parking lots, and all entrance points to all light rail stations. Contact DART Police to verify passenger facilities with surveillance capabilities. The video is recorded on-site at a designated location at high resolution. Video is transmitted to a central monitored location (CML) at DART Police Dispatch. The camera system is monitored by DART Police Dispatch and trained camera monitor personnel. The video may be retrieved at DART Police Dispatch by camera monitors for both on-site archive stations and stations viewed from Police Dispatch. Video will be retained for a period fourteen days and then will be written over.

Mobile surveillance consists of fixed cameras viewing the interior and forward facing view on specified buses and super light rail vehicles. The video is recorded on the vehicle and will allow operators to 'tag' an event with an incident button. Tagged video will be downloaded while at the bus and super light rail operations facility. Tagged video will only be reviewed if an approved request is received. Video that has been requested, but not previously tagged, will be downloaded at the bus operations facility. Video that is not retrieved from the vehicle will be overwritten.

All downloaded video will be in original format. Only video that is retrieved for the attorney general will be converted to windows media format along with the original format. All other requestors are responsible for ensuring their computer has the appropriate software and drivers to run the viewing software.

This does not apply to the Transportation Department Drive Cam Video system.

PROCEDURES:

1. DART personnel must submit written request for any video surveillance files using DART Net Service Request (under Police menu)
 - a. Request must include adequate data to identify an incident such as date, time frame, location (station name and location at station), and description of incident, vehicle number, and route.
 - b. All requests must have a justification.
 - c. Timeframe shall be minimal time necessary to adequately capture event.
 - d. Date of request shall not exceed 14 consecutive days from the event date.
2. Video request must fall under the following categories to receive consideration from DART Police:
 - a. Claim against DART (General Counsel, Risk Management)
 - b. Open Record Request
 - c. Agency with a Criminal Justice Function
 - d. Supervisor request (Tracking employee actions: DART video will NOT be used to track the daily activities of employees for policy compliance UNLESS their activity is also of a criminal nature.)
 - e. Investigation of a reported crime.
 - f. Drive Cam Video request must be requested from Transportation Department only.
3. Requests must be approved by an AVP or above through the Workflow process.
4. If approved, the monitor will search the video storage depository for video file. If the file is found, the monitor will review the file for content and initiate download of the event in 3-5 minute increments that best covers the requested event.
5. Police reserves the right to reject requests for the following reasons:
 - a. Too vague – Requestor did not provide good description of the event
 - b. Invalid Date – Requests video past 14-day limit
 - c. Timeframe too long – Requests appear unreasonable in length
 - d. Event not found – No event found matching request description
 - e. No disclosure – Requestor does not document why his/her department needs the video
 - f. Sensitivity of information – Per Police discretion, video files can be labeled as not distributable for any reason

- g. File corruption – Video file corrupt and cannot be viewed
- 7. Once the file is in the storage server, the requester will be notified. Requestor is responsible for picking up the video within 24 to 48 hours of the completion of the download. Monitor will log all downloaded files and require a signature from the requestor.
- 8. If a video is distributed under this section to a DART Department, the record retention policy of the department receiving the video shall apply.
- 9. All video is for official use only.
- 10. A DART Police Lieutenant, manager or above is authorized to direct immediate video retrieval. Videos retrieved under emergency situations will be reviewed by DART Criminal Investigations Division and General Counsel before release to other departments or agencies.

VIDEO STORAGE:

Any video that is not retrieved, as defined above, within 14 consecutive days of the video, is deemed not to be administratively valuable and may be erased or overwritten. If the requestor fails to provide media storage, any video retrieved that is not transferred to a storage media by DART Police within 14 consecutive days of the video is deemed to not be administratively valuable and may be erased or overwritten.

I approve of this document as Operations policy and procedure for DART Surveillance Video, and appoint DART Police the point of contact for all document updates and changes.

Carol Wise
EVP – Operations

James D. Spiller
Chief of Police

Distribution List:

DART Police
Transportation
Legal Department

Record Number	Record Title	Record Description	Retention Period	Remarks
*GR1000-36	PERMITS AND LICENSES	Records documenting the application for and the issuance of permits and licenses (including certificates of liability and other required documentation) by a local government for sales, solicitation, facility usage, and similar activities. Does not include permits and licenses issued for the construction of or alterations to real property, for those relating to health and sanitation, or for those issued by police or fire departments listed in other commission schedules.	Expiration, cancellation, revocation, or denial + 2 years.	
GR1000-37	PHOTOGRAPHS, IMAGES, RECORDINGS, AND OTHER NON-TEXTUAL MEDIA	Photographs, photographic scrapbooks, slides, sound recordings, videotapes, posters, and other non-textual media that document the history and activities of a local government or any of its departments, programs, or projects except such records noted elsewhere in this or other commission schedules.	AV.	Retention Note: Review before disposal, some records may merit PERMANENT retention for historical reasons. Local governments should consult with local historical or genealogical societies to assist with the appraisal. Be certain that photographs and other non-textual media do not fall within other records series. For example, mug shots and photographs of fire damage are listed in Local Schedule PS (Records of Public Safety Agencies) under police and fire department records respectively.
GR1000-38	POLICY AND PROCEDURE DOCUMENTATION	Executive orders, directives, manuals, and similar documents that establish and define the policies, procedures, rules, and regulations governing the operations or activities of a local government as a whole or any of its departments, programs, services, or projects.	US, expired, or discontinued + 5 years.	Retention Note: Review before disposal; some records may merit PERMANENT or long-term retention for historical or legal reasons.

Record Number	Record Title	Record Description	Retention Period	Remarks
PS4050-05c	WEAPONS RECORDS	Records documenting the sale, gift, loss, or destruction of public safety weaponry.	3 years.	
PS4050-05d	WEAPONS RECORDS	Inventories of weapons.	US + 3 years.	
PS4050-06	SURVEILLANCE VIDEOS	Video surveillance for, but not limited to, security of property and persons.	AV.	
*PS4050-07	GPS TRACKING RECORDS	Global Positioning System (GPS) data used to track locations of a government fleet vehicle when such tracking is part of standard operating procedure.	30 days.	Retention Note: If used as part of an investigation, retain as part of item number PS4075-01 or PS4125-05.
*PS4050-08	PROTECTIVE CLOTHING RECORDS	Includes bullet-resistant and stab-resistant vests, SWAT equipment, fireproof clothing, and other protective and safety wear.		Retention Note: Use GR1075-21 for other personal equipment assigned if it is not listed elsewhere in this schedule.
*PS4050-08a	PROTECTIVE CLOTHING RECORDS	Daily or other periodic reports on the inspection of protective clothing.	3 years.	
*PS4050-08b	PROTECTIVE CLOTHING RECORDS	Inventories of protective clothing.	US.	

SECTION 1-3: PERSONNEL RECORDS





Retention Note: This part supplements and should be used in conjunction with Part 3 of Local Schedule GR (Records Common to All Governments).

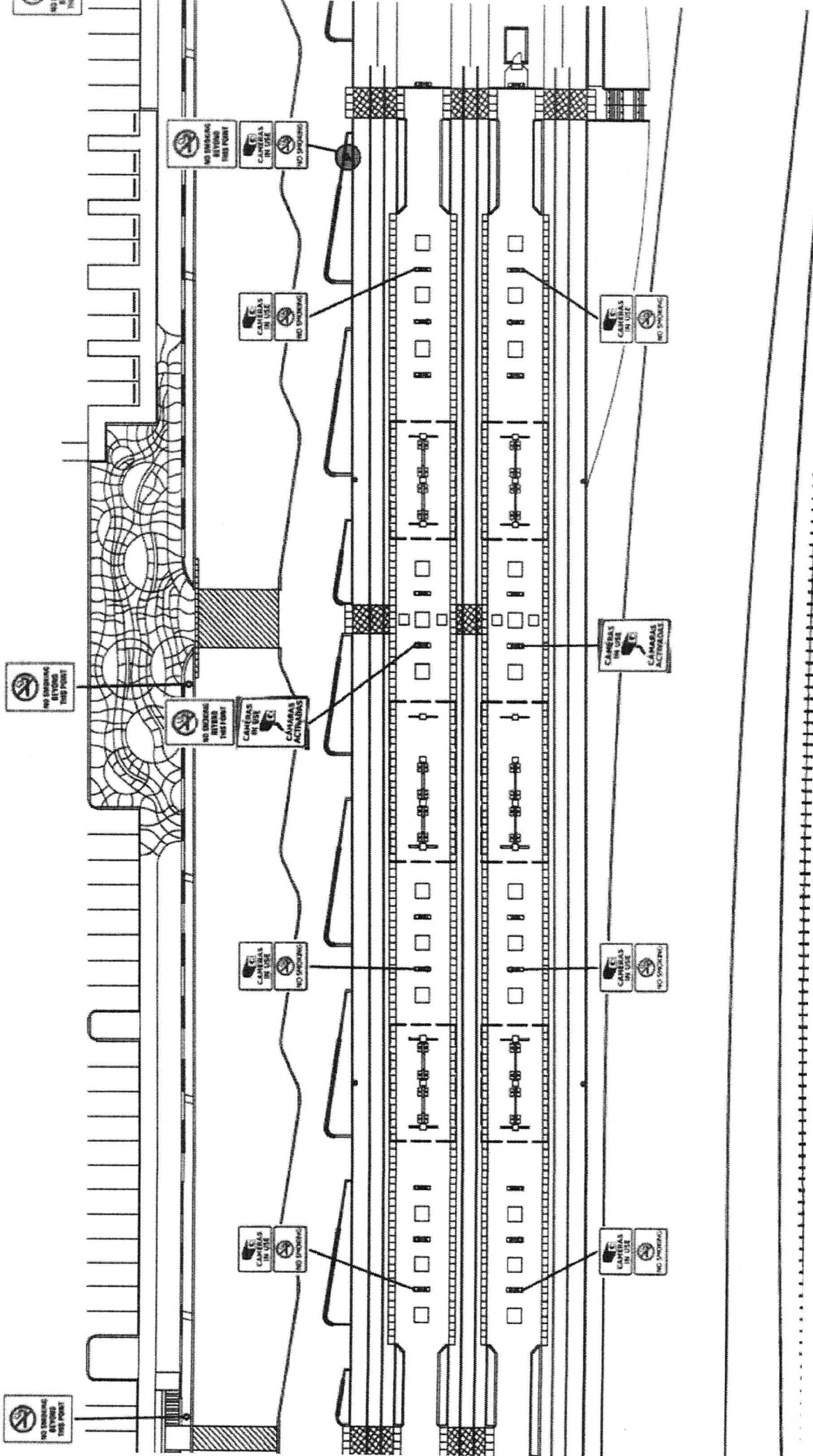
Record Number	Record Title	Record Description	Retention Period	Remarks
*PS4075-01	INTERNAL AFFAIRS INVESTIGATION RECORDS	Records documenting the initiation, investigation, and disposition of internal affairs investigations of alleged misconduct by law enforcement officers, fire department personnel, emergency medical services personnel, and other employees subject to internal affairs investigations.		Retention Notes: a) Retention periods for this record group date from the completion of the investigation. b) Use GR1050-07 for investigations and reviews conducted by a Firefighters' and Police Officers' Civil Service Commission.
PS4075-01a	INTERNAL AFFAIRS INVESTIGATION RECORDS	Records of investigation of law enforcement shooting incidents that result in death or injury to any person, including a police officer.	PERMANENT.	

Record Number	Record Title	Record Description	Retention Period	Remarks
*PS4125-02	ARREST REPORTS	Arrest reports and fingerprints for each person arrested by the law enforcement agency and charged with a felony or a misdemeanor. (1) Class C misdemeanors and unclassified violations of state law or local ordinance punishable by fine only. (2) All other offenses.	6 months. 75 years, or date of death of individual, if known, whichever sooner.	Retention Note: If the arrest report lacks any information listed in Code of Criminal Procedure §60.051(a)(1)-(3) and (b)(1), (3)-(8), documents from PS4125-05 sufficient to provide the missing information must be kept for as long as the retention period of this series. If the person arrested is a juvenile, the law enforcement agency should use item numbers PS4225-06, PS4225-08, or PS4225-10.
*PS4125-03	BAIL BOND RECORDS	Record of bail or recognizance bonds taken by a sheriff or other peace officer pursuant to Code of Criminal Procedure. §§17.20-17.22 and as required by §17.39.	3 years; or 3 years after last entry if in bound volume.	
*PS4125-04	VIDEO AND AUDIO RECORDINGS	Video or audio recordings captured by police officers or as part of an automated enforcement program.		For security camera videos, see GR1075-25.
*PS4125-04a	VIDEO AND AUDIO RECORDINGS	Video or audio recordings from police vehicles of persons on whom charges are not filed.	90 days after the date of the stop.	By law - Code of Criminal Procedure §2.135(b)
*PS4125-04b	VIDEO AND AUDIO RECORDINGS	Video or audio recordings from police vehicles of persons on whom charges are filed or related to an administrative investigation of an officer.	Follow retention period for item number PS4125-05b if charges filed or item number PS4075-01 if officer subject to internal affairs investigation.	By law - Code of Criminal Procedure §2.135(b).
*PS4125-04c	VIDEO AND AUDIO RECORDINGS	Red-light camera videos that do not capture a violation, or for which a notice of violation is not mailed.	30 days.	By law - Transportation Code §707.011(b).

Record Number	Record Title	Record Description	Retention Period	Remarks
*PS4125-04d	VIDEO AND AUDIO RECORDINGS	Red-light camera videos that capture a violation.	Date civil penalty paid or 31 days after judgment, whichever sooner.	By law - Transportation Code §707.016.
*PS4125-04e	VIDEO AND AUDIO RECORDINGS	Officer-worn camera videos that do not capture a violation, use of deadly force by an officer, or are otherwise unrelated to an administrative or criminal investigation of an officer.	90 days.	By law - Occupations Code §1701.655(b)(2).
*PS4125-04f	VIDEO AND AUDIO RECORDINGS	Officer-worn camera videos that capture use of deadly force by an officer, are otherwise related to an administrative or criminal investigation of an officer, or capture a violation by any person.	Follow retention periods for items PS4075-01 or PS4125-05, as appropriate, but not less than 90 days.	By law - Occupations Code §1701.660(a).
*PS4125-05	OFFENSE INVESTIGATION RECORDS	Offense and supplemental offense reports; investigation reports and notes; witness statements; latent fingerprints; results of chemical analysis and polygraph tests; crime scene, mug shot, and other photographs; laboratory reports; arrest reports (Class C misdemeanors only); citations; affidavits; criminal processes; victim impact statements; subpoenas; and other records of a law enforcement agency relating and customary to the investigation of criminal offenses or other violations of state law or local ordinance.		
PS4125-05a	OFFENSE INVESTIGATION RECORDS	Cases not cleared.	Until the statute of limitations has expired.	By law - Code of Criminal Procedure, Chapter 12.

LEGEND:

-  SIGN TYPE 1 - FACING AHEAD
-  SIGN TYPE 2 - FACING TRUCK
-  EXISTING "CAMERAS IN USE"
-  POLE LOCATION



Number TOS-1006	Subject Event Recorder	Effective Date November 16, 2015	Revision 1
---------------------------	----------------------------------	--	----------------------

STANDARD OPERATING PROCEDURE

DALLAS AREA RAPID TRANSIT

TRANSPORTATION DEPARTMENT

Event Recorder

REVISION	DATE	DESCRIPTION	INIT
	7/18/2014	Initial Release (TOS-1006 SMARTDrive)	ME
1	11/16/2015	Changed title; complete minor changes to procedures	ME

ORIGINATED BY: Jose Carranza DATE: 11-12-2015
Jose Carranza, Senior Manager, Bus Operations

APPROVED BY: Monica Ellington DATE: 11/11/2015
Monica Ellington, Manager, Transportation Services

APPROVED BY: Maurice Bell DATE: 11-12-15
Maurice Bell, Assistant Vice President, Bus Operations

APPROVED BY: Wanda Schafer DATE: 11/12/15
Wanda Schafer, Assistant Vice President, Transportation Services

APPROVED BY: Tim Newby DATE: 11/17/2015
Tim Newby, Vice President, Transportation

Number TOS-1006	Subject Event Recorder	Effective Date November 16, 2015	Revision 1
---------------------------	----------------------------------	--	----------------------

Table of Contents

PURPOSE.....	3
REFERENCE.....	3
DEFINITIONS.....	3
PROCEDURAL OVERVIEW.....	3
PROCEDURE	4

Attachment

SMARTDRIVE RETRIEVAL FORM	7
--	----------

Number TOS-1006	Subject Event Recorder	Effective Date November 16, 2015	Revision 1
---------------------------	----------------------------------	--	----------------------

Purpose

The purpose of this Standard Operating Procedure (SOP) is to establish a standard for appropriate use of video information that may be captured by the event recorder system, as well as establishing procedures for responding to Open Records Act requests for Transportation related video information.

Reference

Bus Operator Rule Book

DART Hourly Employment Manual (HEM)

Definition

- Safety Infraction - Any incident which occurs while the bus is in motion that violates DART's rules and policies, e.g. speeding, failing to stop at railroad crossing, operating a cell phone while in the driver's compartment of the bus, etc.
- Triggered Events – Recorded video segments that are captured by the event recorder system and forwarded to DART management staff.
- Tagged Events – Recorded video segments obtained at the operator's request based upon the operator pushing the 'panic' button.

Procedural Overview

In an effort to increase the overall safety of DART's system, the event recorder system is installed on all new revenue vehicles. The camera system records events which may be worthy of counseling, as well as those which may warrant corrective or disciplinary action due to a violation of DART policy. Upon the installation of the event recorder system in 2012, it was communicated that management would provide a grace period of six (6) months during which the event recorder information would be used for coaching, but not for corrective or disciplinary action, except in the case of an accident or significant safety violation. The grace period is no longer in effect. Therefore, this SOP addresses the actions which may be taken to address events captured on video.

Number TOS-1006	Subject Event Recorder	Effective Date November 16, 2015	Revision 1
---------------------------	----------------------------------	--	----------------------

The event recorder system includes on-board event recorder equipment together with computer software used in reviewing and tracking recorded incidents. It consists of fixed cameras that capture images/audio inside and outside the bus. The camera focused inside the bus captures the passenger cabin, front door area and the operator's seating area. The camera focused outside the bus captures the view outward from the front windshield.

The cameras will record triggered video events (for a specific number of seconds prior to and after a triggered event). Once the system acknowledges the trigger, an event is saved and forwarded to operations management staff. An Operator may manually create a tagged event, which will be saved and forwarded to a member of the operations management staff.

Operations staff will monitor the triggered video events and provide opportunities for Supervisors and Managers to coach Operators on techniques to operate vehicles more safely or initiate corrective or disciplinary action should there be violations of DART policies or procedures.

Procedure

A. Appropriate Use

1. Video evidence may be retrieved based on precipitating events including, but not limited to:
 - a. Investigation of accidents/incidents including safety-related infractions;
 - b. Reports/allegations of criminal activity including tampering with on-board security camera systems;
 - c. Reports/allegations of injury to employees or customers;
 - d. Reports of damage to DART systems/facilities;
 - e. Investigation of Priority 1 customer complaints (e.g., unsafe operation, dispute with customer, rude/discourteous behavior, unacceptable conduct);
 - f. Reports or observations of employee use of personal electronic devices while in the driver's seat of a bus;
 - g. Use as a training tool.
2. Video requests from DART Management will be for business purposes only. Any audio or video record of personnel shall not be used by any manager in a manner that would be obvious to be "targeted surveillance" or "fishing" except where there is an initiating event such as those listed in items above (a-g).

Number TOS-1006	Subject Event Recorder	Effective Date November 16, 2015	Revision 1
---------------------------	----------------------------------	--	----------------------

B. Video Viewing & Control

The event recorder system is monitored by the external vendor. This system is constantly capturing images based upon preset criteria provided by DART. Video from the cameras will be maintained for a period of fourteen (14) days and then will be written over.

1. DART staff with viewing capabilities may not share video without approval of the division Senior Manager.
2. When viewing rights are administered, the division Senior Manager will specify who the videos may be shared with.
3. To retrieve a video copy, DART Management personnel must submit a written request to SMARTDrive using the incident retrieval form. (see Attachment 1)
4. Vendor will forward the video requested.

C. Open Record Requests

This standard applies only to Open Records Request received by the Public Information Officer (PIO) and forwarded to Transportation. For video related requests, this standard applies only to video obtained through the event recorder video system. All downloaded video will be in original format. Requestors are responsible for ensuring their computer has the appropriate software and drivers to run the viewing software.

1. Authorized Transportation staff will be notified through the Public Information Process of such request. The Transportation Analyst or alternate is responsible for research of the requested video. The following information should be included in the request:
 - a. Adequate data to identify an incident: date, time, specific location, vehicle number (when possible), route and description of the incident.
 - b. The requested time of the incident must be minimal to adequately capture a specific event.
 - c. Date of requests shall not exceed fourteen (14) days from the event date.
 - d. If a request for video does not contain sufficient information, the PIO will be contacted to seek clarification of the request.

Upon retrieval of the video, it will be uploaded thru the Public Information Process to route to the requestor.

Number TOS-1006	Subject Event Recorder	Effective Date November 16, 2015	Revision 1
---------------------------	----------------------------------	--	----------------------

D. Training

Training for event recorder was initially performed through 'train the trainer' methods. The Assistant Manager, Service Assessment Operations, provided the required training for all transportation staff. Any subsequent training has been provided to new staff by division staff. Also, the Assistant Manager is available to provide any additional training as requested.

E. Safety & Risk Management

Safety is of primary importance in carrying out DART duties and responsibilities. Use of the event recorder technology is essential in correcting risky and/or poor driving behaviors. This system will also exonerate employees from false allegations by showing proof when the employee does everything possible to prevent a situation on the bus. This system will also aid in preventing altercations with the Bus Operators. Bus Operators are the primary targets with regard to passenger assaults. The event recorder helps to identify perpetrators if triggered during a physical altercation on the Bus Operator resulting in bringing the perpetrator to justice.

From a risk management vantage point, this system will protect the company from false claims. Many times in the transportation business, stories are shared about passengers claiming false injuries when using public transportation. Having the event recorder system record these events will clearly exonerate the agency and prevent payment on those false claims.

The division Safety Specialist will work with operations staff to collect information regarding any safety violations which take place on or around the bus.

F. System Maintenance

System Maintenance will be performed as needed based upon information supplied on the bus defect cards or reports from the event recorder vendor.

Number TOS-1006	Subject Event Recorder	Effective Date November 16, 2015	Revision 1
---------------------------	----------------------------------	--	----------------------

Attachment 1

SMARTDRIVE

Incident Retrieval Form

Please complete the form below and email it to customer.service@smartdrive.net.

Due to amount of research associated with Event Retrievals, it may take up to 24 hours to provide you with a definitive response. If you have any questions or would like to check the status of your request, please find your Service Case number and contact *Technical Support at 1-866-933-9930*.

*Requestor Name		*Requestor Title
*Company Name	*Site Name	*Today's Date

*Date of incident	*Time of incident	*Location of incident (Address and/or nearest cross street)
-------------------	-------------------	---

1. *Please complete the following:

*Vehicle serial number	*SmartRecorder serial number
*Vehicle Identification Number (VIN)	*Driver (First and Last Name)

2. *Type of incident:

--- Please select one ---



Please specify if you selected "Other" in the box above:

3. *Please attach photos of the damage to the vehicle, other vehicle and/or fixed object along with this form.

NOTE: We request photos to assist us in understanding the forces exerted on the vehicle and subsequently the SmartRecorder. This provides context as we evaluate the performance of the SmartRecorder around the time of the incident. Without photos, we may be limited in our ability to fully address your request.

4. *Detailed description of incident.

5. *Were there any injuries to the vehicle occupants?

6. Please provide any additional comments.

SMARTDRIVE PROPRIETARY AND CONFIDENTIAL

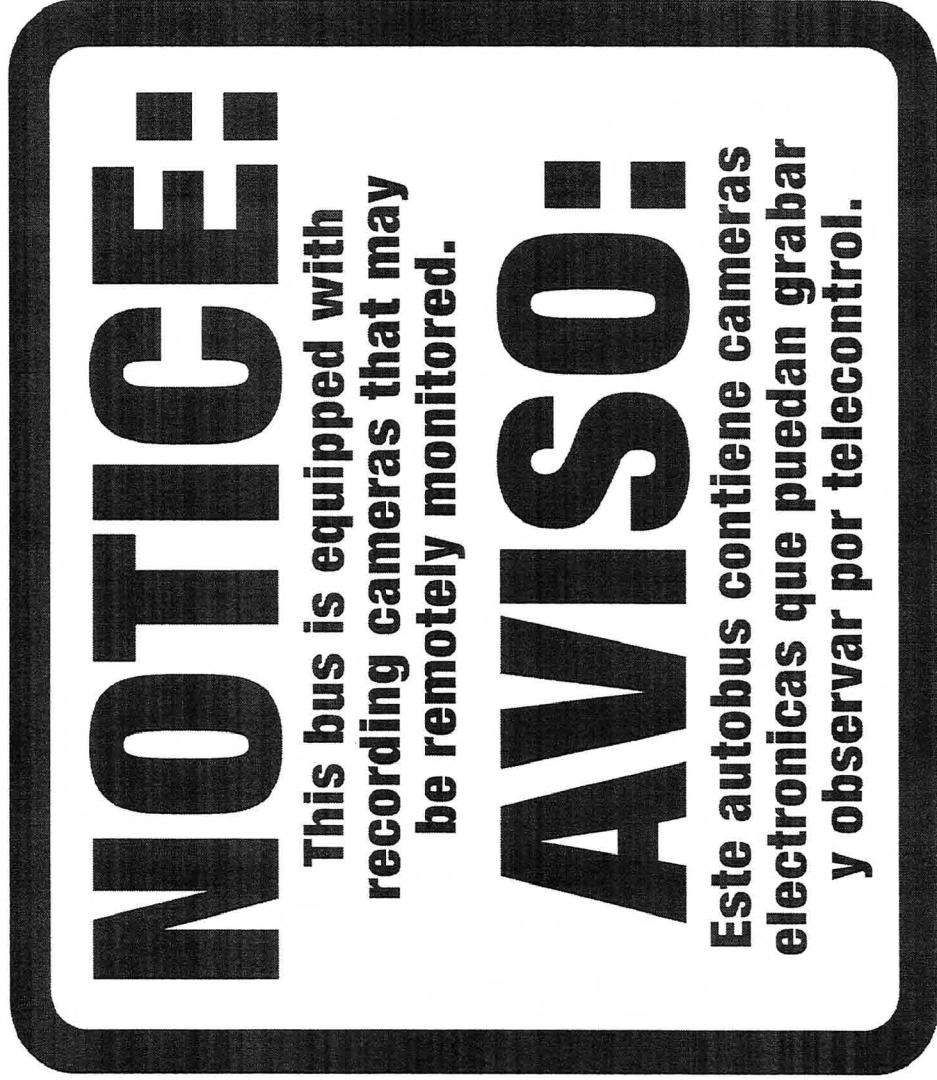
DART Surveillance Decal/Bus



DART Sign Type Surveillance Decal/Bus
Scotchcal 3M 3650-10 White
Copy and Border: PMS 281C Blue

5" X 6" .25" Corner Radius

5.5 inches



5 inches

NABI & ARBOC Interior Security Camera Decal
5" x 7"; Black on white non-glare vinyl.
Keyline does not print

Notice:

**This bus is equipped
with recording cameras
that may be remotely
monitored.**



Aviso:

**Este autobús está equipado
con cámaras de video que
pueden ser monitoreadas
en forma remota.**



Note: keyline for reference only, does not print



Sign Standards Manual

12" x 16" Black on selective white
0.125" thick aluminum
.25" white border with .25" black inline border
Silkscreen per DART Specifications NSF-2405



Note: Keyline for reference only, does not print



Sign Standards Manual

12" x 18" Black and Red on reflective white
0.125" thick aluminum
.25" white border with .25" black inline border
Silkscreen per DART Specifications NSF-2405

Duluth Transit Authority

Surveillance Video Control Policy

General Access Policy

Controlling access to video equipment, view stations and data files are a company priority. As a matter of company policy no camera, DVR, saved data file or other related equipment may be accessed without specific authorization by DTA management. All DVR's for buildings and buses must be stored in a secured and limited access area. Personnel must have authorization by the Director of Safety & Training, Director of Maintenance, Director of IT or the General Manager to access DVR and camera equipment. Unauthorized access or removal of equipment or data files from DTA property is prohibited. Failure to follow this policy is a violation of DTA Security Policy and subject to disciplinary action including termination of employment.

Confidentiality

As a matter of policy all retained video and audio data files are confidential and are property of the DTA. Under no circumstance shall an employee share information regarding any saved video of an incident, accident, customer service event, crime, etc. without specific authorization from Company management..

Privacy

Video data is a tool used by DTA as a method for investigating crime, customer service incidents, traffic, passenger accidents, vehicle accidents and safety policy violations. Video data is considered confidential and must be maintained in a matter that is secure and accessible only to designated staff investigators and involved employees.

All retrieved data hard drives, DVD copies and photographs derived from data files must be held in a secure area. Incident view stations must be located in a private and secure area. Unauthorized personnel, members of the general public, media, etc. may not view video data files unless authorized by the General Manager or designate.

Sharing information about the content of incident data files with unauthorized persons is a violation of this policy.

Law Enforcement

Video data is a proven method for deterring and investigating crime. As a matter of policy DTA cooperates with local law enforcement officials by providing access to video data files. Authorized staff may furnish data files to law enforcement when requested for a specified incident. No other files may be released.

Media

The Minnesota "Governmental Sunshine" Law allows for media and other interested parties to obtain certain documents and data files from governmental agencies. It is the policy of DTA not to release any data file to media or outside entities without the

approval of the General Manager. Requests by media or others for DTA video data files must be forwarded to the General Manager who is authorized to grant or deny the request.

Staff Control

General Manager - The General Manager has the authority to access all video equipment and data files. The General Manager may also designate DTA staff as an agent for management of this program.

The General Manager has authorized the Director of Safety and Training to manage the Surveillance Video Program. Duties include but are not limited to ---

- Assuring the system is operational and maintained,
- Assuring only authorized personnel has access to equipment and saved videos,
- Saved video data files are retained in an orderly, controlled, secure and confidential manner,
- Saved videos are released to outside entities in accordance with policy approved by the General Manager,
- Authorized staff has received the necessary training for the operation and maintenance of equipment.

The Director of Safety and Training is authorized to access all video equipment and saved data files.

Operations Supervisor - The Operations Supervisor has the authority to obtain video data sourced from buses and the building surveillance systems. Authorizations also include viewing, saving, cataloguing, reviewing saved data files with appropriated staff and providing saved data files to authorized outside entities.

Dispatcher - The Dispatcher has the authority to request the retention of bus video data files and forward to appropriate personnel. Dispatchers are not authorized to view data files or provide information of a data file to unauthorized persons. One Dispatcher is designated and authorized to access data files for monthly maintenance checks.

Maintenance Personnel - Designated Maintenance personnel are authorized to maintain equipment and have limited access to data files. Maintenance personnel may not save or retain data or share information regarding a data file unless specifically authorized to do so by the Director of Maintenance, General Manager or Director of Safety.

Director of Information Technology (IT) - The Director of IT has the authority to retain and view data files as necessary for the maintenance of the system. The Director of IT may not share information regarding a data file unless specifically authorized by the General Manager or Director of Safety & Security.

Video Data File Retention Policy

Data files are saved on a secure server maintained by the IT Department. The secure server is double password protected and may only be accessed by authorized staff. DTA staff are required to use DTA approved user and passwords to access DVR data files for viewing and saving data files.

Procedures for Obtaining, Viewing and Saving Video Data Files

Bus Videos

- Request form is completed and forwarded by Supervisor to Dispatcher ordering retention of DVR data.
- Maintenance Personnel, Operations Supervisor, or the Director of Safety retrieves DVR data.
- DVR data is viewed on password protected secure viewing equipment.
- Event is located and determination is made to retain event file.
- File is downloaded from hard drive to secure DTA server file.
- Event file is labeled using a specific naming protocol which includes date of incident, bus number, operator number, and database incident number associated with written incident report.
- Physical hard drive is released and returned to bus, or original uploaded video file is deleted from Verint and Nexus systems.
- Still photographs may be printed from stored event files
- Event files can be stored on a DVD and provided to an authorized outside entity.

Building Videos

- Request form is completed and retained by Supervisor.
- Video is reviewed on any so-equipped work station.
- Data files are saved and/or copied to DVD.

Equipment

Surveillance video equipment is installed and active DTA in the following locations:

All DTA revenue vehicles - from 3 to 8 cameras depending on vehicle
DTA Operating Facility - 16 cameras, 1 DVR
Duluth Transportation Center – 65 cameras, 2 DVRs
Transit Center East - 8 cameras, 1 DVR
Holiday Bus Stop - 2 cameras, Shared DVR at Transit Center East
Medical Center 3rd Ave. East - 6 cameras, 1 DVR
One Portable Camera, DVR

Monitoring stations are located in the Dispatch Office in the DTA Operating Facility, Sales Booth within the DTC, DPD substation in DTC, and Director of Operations office. These stations are monitored during all staff hours. There are additional unmonitored stations located in the Safety Office, Maintenance Office, IT Server Room and 3rd

Avenue East. View stations are located in the Operations Supervisor's Office, IT Server Room and Maintenance Department.

Maintenance of Equipment

Surveillance video equipment is maintained by the DTA Maintenance Department, IT Department and contracted vendors when necessary. The Maintenance Department is responsible for Maintenance of DVR hardware and cameras. The IT Department provides maintenance for software, IT network applications and operational support. Preventative maintenance checks for all Safety View bus equipment is completed monthly by the morning dispatcher. PM checks for the Verint and Nexus systems are conducted whenever an Operations Supervisor uploads and views a video, which is almost daily. Both systems are self-monitoring, and will indicate any problems with any cameras on any bus within the system when the software is used. PM checks are made for sound levels and clarity, camera operation, aiming and focus, and timekeeping. All systems will also indicate any problems to the operator after start-up when the pre-trip is being conducted. The operator is to report any issues to dispatch and/or maintenance immediately, before they leave the garage. Any problems that are detected during the PM are conveyed to the maintenance department by email. All problems are corrected as soon as possible by maintenance. A bus with a significant video system problem is taken out of service until repair of the problem can be completed.

Preventive maintenance checks for building equipment located at the DTA Operating Facility and Duluth Transportation Center-Transit Center East are made daily. Equipment located at 3rd Avenue East is checked weekly. Equipment is checked for camera positioning and video quality. Records of these maintenance checks are completed and maintained in the Safety Office. All defects are reported to the Maintenance or IT Departments for repairs.

All outside contractors who are employed by the DTA for system maintenance or repair are covered by this policy as well.

Revised April, 2017

Prepared by Safety & Training Department

**FOR YOUR SAFETY AND
SECURITY THIS BUS MAY
BE UNDER AUDIO/VIDEO
SURVEILLANCE**

Escambia County Area Transit, Pensacola, Florida

Attachment re Bus Audio/Video Surveillance System to current Labor
Agreement between ATU Local 1395 and Escambia County Area Transit

26

ATTACHMENT



Addendum to the current Labor Agreement between ATU Local 1395 and Escambia County Area Transit dated March 1, 2002 – February 28, 2005 for the Bus Audio/Video Surveillance System.

Purpose: To explain the Escambia County Area Transit “Bus Audio/Visual Surveillance Policy/Procedures” and to inform all employees about the Bus Audio/Visual Surveillance System and provide information to assist all employees in understanding their rights and responsibilities under the policy/procedures.

Scope: This policy is subject in all respects to all future and present applicable laws, statutes, ordinances and regulations that pertain to audio/visual surveillance systems.

This policy will provide information concerning training, operation and uses for the bus audio/visual surveillance system on Escambia County Area Transit vehicles.

Training:

Initial Training:

- Will be provided to all current bus operators and operations supervisors concerning the operation of the system on the vehicle.
- New operators will receive initial training on the system during their bus operator-training period.

Refresher Training:

- Will be provided to all operators on a case by case basis.
- Will be provided to all operators should there be a change in the system that would effect the operation of the system for the operator.

System Operation:

Pre-Trip Inspection:

- Inspect all camera pods for physical damage and secure mounting.
- Ensure all camera pod lenses are clear of any obstruction that would prevent the recording of images.
- Inspect the audio microphone pod for physical damage and secure mounting.
- Ensure the microphone is clear of any obstruction that would prevent the recording of audio onboard the vehicle.
- Ensure the door for the digital video recorder (DVR) unit is closed and locked (if not, notify dispatch for further instructions).

NOTE: Do not leave the garage area if door to the digital video recorder (DVR) unit is not closed and locked.

- Ensure the system status light is GREEN (If not green notify dispatch for further instructions).

Addendum Bus Audio/Video Surveillance System Page 2

Surveillance System Operation while Vehicle Is In Service:

- The operator will be responsible to monitor the system status light to ensure the system is functioning (should the system status light indicate that the system is not operating notify the dispatcher for further instructions).
- When checking the vehicle for items left by passengers check the camera pod lenses for obstructions that would prevent the recording of images.
- In the event of a collision the system will automatically tag the event.
- In the event of a disturbance on the vehicle the operator should press the surveillance system panic button to tag the event and notify the dispatch office.

Recorded Audio/Video Surveillance Data Uses:

The primary purpose of having an audio/video surveillance system on the buses is operator and passenger security.

Pictures from recorded data may be posted on bulletin boards for training and awareness of all operators (pictures may not include the image of the operator involved in the incident).

Accident Investigations:

- Recorded data may be reviewed to gather facts to assist in determining if the accident was preventable or non-preventable.
- Recorded data may be utilized in legal proceedings as evidence.
- Recorded data may be utilized to assist in identifying a vehicle in a hit and run type of accident.
- Should inappropriate behavior on the part of the operator be observed/heard, during the review of the recorded data for an accident investigation, the operator may be subject to progressive discipline?

Passenger Accidents/Incidents:

- Recorded data may be used to identify passengers that were involved in an accident/incident (i.e. assaults, vandalism, harassment, crimes, etc.).
- Recorded data may be provided by Escambia County Area Transit to our insurance carriers to assist them in fact finding to determine liability.
- Recorded data may be reviewed to gather facts to assist in determining if a passenger accident/incident was preventable or non-preventable.
- Recorded data may be reviewed to determine the validity of complaints alleged by passengers against operators.
- Recorded data may be reviewed to determine the validity of complaints alleged by operators against passengers.
- Should inappropriate behavior on the part of the operator be observed/heard, during the review of the recorded data for a passenger accident/incident investigation, the operator may be subject to progressive discipline?

Addendum Bus Audio/Video Surveillance System Page 3

Complaints:

All Complaints received will be recorded on the ECAT Record of Complaint form. The employee receiving the complaint will complete the form providing as much information as he/she can obtain from the complainant. The Complaint Form should have, if possible, the complainant's name, address, and phone number. Inform the complainant that this information is necessary in order for the ECAT staff to obtain additional information if required by an investigation, and that ECAT may not be able to complete a through investigation of anonymous complaints.

- Appropriate ECAT personnel will review the complaint, and determine if the complaint is of a serious or non-serious nature. After reviewing the complaint, and if it is determined to be a non-serious complaint, the Company will note the complaint as a non-serious complaint. This will not require any further action involving discipline, or reviewing the Audio/Video Surveillance System, however the appropriate supervisory personnel may interview the employee involved to discuss the incident for the purpose of informing the employee of a possible problem area.
- If the complaint is determined by the Company to be a serious complaint, the Company will thoroughly investigate the incident, and may include the recorded data of the Audio/Visual Surveillance System to determine the validity of the complaint alleged against the operators and/or operators against passengers.
- All complaints must be in writing on the Company "Record of Complaint Form." The name, address and/or phone number of the person with the complaint (if obtainable) will be on the "Record of Complaint Form." The Company will provide the Union with a copy of the complaint upon request.
- Should the viewing of the recorded data provide clear evidence of no wrong doing on the part of the operator/passenger the complaint will be so annotated and the complaint will not be brought to the attention of the operator/passenger.

- Should the Company decide that inappropriate behavior on the part of the operator is observed/heard during the review of the recorded data for a complaint investigation, the operator may be subject to progressive discipline. The Union may view the recorded data after complying with the procedures in this agreement for Union viewing of recorded data. The Company will provide the Union with a copy of the involved data on a CD provided by the Union for this purpose.

Addendum Bus Audio/Video Surveillance System Page 4

- Should inappropriate behavior on the part of the passenger be observed/heard during the review of the recorded data for any complaint, the Company will take appropriate action with the passenger.
- The Company does not intend to use the Audio/Visual Surveillance System as a method of randomly checking operator performance, and will not normally use the system to verify anonymous complaints against an operator, however, the Company reserves the right to use all information obtainable, including the Audio/Visual Surveillance System, to investigate any complaint, even if anonymous. All complaints, even anonymous complaints, that are determined be serious enough to affect the safety of passengers and equipment, or could result in legal action against ECAT, could result in progressive discipline. The Company agrees that if an anonymous complaint results in a review of the Audio/Visual Surveillance System, the Audio/Visual information must show clear evidence of wrong doing by the operator in order for progressive discipline is taken on the operator.

Operator Viewing of Recorded Data:

- Operators may request to view recorded data during the time they were operating a vehicle.
- A Company representative will assist the operator in viewing the recorded data.
- ECAT may not permit another operator to view another operator's recorded data even if the operator whose data is viewed gives their permission.
- Operators must request in writing to view such recorded data not later than five (5) calendar days from the day to be viewed. The request is to be submitted on the Operator Audio/Visual Viewing Request Form (provided by the company).
- Operators must view the recorded data when it does not interfere with their normal work assignments and they are in a no pay status.

Union Viewing of Recorded Data:

- A Union official may request in writing to view recorded data with the written permission of the operator of the vehicle on the date and time the data was recorded. The request must be made not later than five (5) calendar days after the day to be viewed, on the Union Audio/Visual Viewing Request Form (provided by the company).
- A Company representative will assist the Union official in viewing the recorded data.

- The Union official must view the recorded data when it does not interfere with their normal work assignments and they are in a no pay status or if the union official is on union business time.

Addendum Bus Audio/Video Surveillance System Page 5

Audio/Video Surveillance System Data Disclaimers:

All audio/video recorded data is the sole property of Escambia County Area Transit and may be made available to any insurance company, law enforcement or judicial system that may have interest in such recorded data. The recorded data may be made available to Amalgamated Transit Union Local 1395 as provided herein this addendum.

The Company hereby agrees that no Audio/Video Surveillance System recorded data will be monitored by the Company or any hired surveillance company or personnel other than as indicated in this addendum.

The Company agrees that the ATU Local 1395 will not assume any responsibility for the accuracy of information obtained by the Company through the use of the Audio/Video Surveillance System.

The Company further will guard the Union of any liability by employee(s) or any other entity as a result of the Company's use of the Audio/Video Surveillance System to the extent permitted by all applicable federal, state and local laws.

**Greater Attleboro Taunton Regional Transit Authority (GATRA),
Taunton, Massachusetts**

Use of Technology in Contract with ATU 1547, Article 24

27

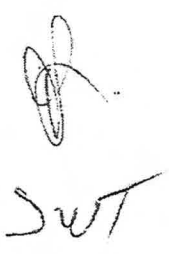
ARTICLE 24 – USE OF TECHNOLOGY

Current technology equipment, and as they may further develop, shall not be used by the Company in a random, retaliatory, and/or discriminatory manner. The Company shall not use such recordings for driver training purposes without the written consent of the employee and others involved. The Company shall allow the Union and affected employees to review such recordings that may result in an employee being disciplined, during normal working hours, as necessary. Upon request the Company shall provide a copy of such recordings, within five (5) business days to the President/ Business Agent, for the Union's use in grievance and disciplinary matters.

The Company may view audio and video recordings or monitor and review other audio transmissions and data recorded by the voice/data communications system for a bona fide reason and after review may discipline a driver as appropriate. A bona fide reason is any work related incident, accident or event which is contrary to the best interest of the Company. If any changes are made to the video when cases are submitted or audio software, the Company shall notify the Union ATU 1547 immediately.

Discipline for customer complaints

Upon investigation the Company may issue discipline based upon the customer complaint and the Union and the employee are entitled to receive the customer complaint with the contact information redacted and view the video. A copy of the video will be provided to the union when the Union requests arbitration.

Handwritten signature and initials, possibly "SWT", located in the bottom right corner of the page.

Go Raleigh Transit (GoRaleigh), Raleigh, North Carolina

N.C. Gen. Stat., Ch. 15A, Art. 16, Electronic Surveillance

28

Article 16.
Electronic Surveillance.

§ 15A-286. Definitions.

As used in this Article, unless the context requires otherwise:

- (1) "Aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed.
- (2) "Attorney General" means the Attorney General of the State of North Carolina, unless otherwise specified.
- (3) "Aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.
- (4) "Chapter 119 of the United States Code" means Chapter 119 of Part I of Title 18, United States Code, being Public Law 90-351, the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986.
- (5) "Communications common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) of Title 47 of the United States Code.
- (6) "Contents" when used with respect to any wire, oral, or electronic communication means and includes any information concerning the substance, purport, or meaning of that communication.
- (7) "Electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than:
 - a. Any telephone or telegraph instrument, equipment, or facility, or any component thereof:
 1. Furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by the subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or
 2. Being used by a provider of wire or electronic communication service in the ordinary course of its business or by an investigative or law enforcement officer in the ordinary course of the officer's duties.
 - b. A hearing aid or similar device being used to correct subnormal hearing to not better than normal.
- (8) "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce but does not include:
 - a. Any wire or oral communication;
 - b. Any communication made through a tone-only paging device; or
 - c. Any communication from a tracking device (as defined in section 3117 of Title 18 of the United States Code).

- (9) "Electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications.
- (10) "Electronic communication system" means any wire, radio, electronic, magnetic, photooptical, or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the storage of such communications.
- (11) "Electronic surveillance" means the interception of wire, oral, or electronic communications as provided by this Article.
- (12) "Electronic storage" means:
 - a. Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
 - b. Any storage of such communication by an electronic communication service for the purposes of backup protection of the communication.
- (13) "Intercept" means the aural or other acquisition of the contents of any wire, oral, or electronic communication through the use of any electronic, mechanical, or other device.
- (14) "Investigative or law enforcement officer" means any officer of the State of North Carolina or any political subdivision thereof, who is empowered by the laws of this State to conduct investigations of or to make arrests for offenses enumerated in G.S. 15A-290, and any attorney authorized by the laws of this State to prosecute or participate in the prosecution of those offenses, including the Attorney General of North Carolina.
- (15) "Judge" means any judge of the trial divisions of the General Court of Justice.
- (16) "Judicial review panel" means a three-judge body, composed of such judges as may be assigned by the Chief Justice of the Supreme Court of North Carolina, which shall review applications for electronic surveillance orders and may issue orders valid throughout the State authorizing such surveillance as provided by this Article, and which shall submit a report of its decision to the Chief Justice.
- (17) "Oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but the term does not include any electronic communication.
- (18) "Person" means any employee or agent of the United States or any state or any political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.
- (19) "Readily accessible to the general public" means, with respect to a radio communication, that the communication is not:
 - a. Scrambled or encrypted;
 - b. Transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of the communication;
 - c. Carried on a subcarrier or other signal subsidiary to a radio transmission;

- d. Transmitted over a communications system provided by a common carrier, unless the communication is a tone-only paging system communication; or
 - e. Transmitted on frequencies allocated under Part 25, Subpart D, E, or F or Part 94 of the Rules of the Federal Communications Commission as provided by 18 U.S.C. § 2510(16)(E).
- (20) "User" means any person or entity who:
- a. Uses an electronic communications service; and
 - b. Is duly authorized by the provider of the service to engage in the use.
- (21) "Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and the term includes any electronic storage of such communication. (1995, c. 407, s. 1; 1997-435, s. 1.)

§ 15A-287. Interception and disclosure of wire, oral, or electronic communications prohibited.

- (a) Except as otherwise specifically provided in this Article, a person is guilty of a Class H felony if, without the consent of at least one party to the communication, the person:
- (1) Willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.
 - (2) Willfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:
 - a. The device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communications; or
 - b. The device transmits communications by radio, or interferes with the transmission of such communications.
 - (3) Willfully discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through violation of this Article; or
 - (4) Willfully uses, or endeavors to use, the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this Article.
- (b) It is not unlawful under this Article for any person to:
- (1) Intercept or access an electronic communication made through an electronic communication system that is configured so that the electronic communication is readily accessible to the general public;
 - (2) Intercept any radio communication which is transmitted:

- a. For use by the general public, or that relates to ships, aircraft, vehicles, or persons in distress;
 - b. By any governmental, law enforcement, civil defense, private land mobile, or public safety communication system, including police and fire, readily available to the general public;
 - c. By a station operating on any authorized band within the bands allocated to the amateur, citizens band, or general mobile radio services; or
 - d. By any marine or aeronautical communication system; or
- (3) Intercept any communication in a manner otherwise allowed by Chapter 119 of the United States Code.

(c) It is not unlawful under this Article for an operator of a switchboard, or an officer, employee, or agent of a provider of electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of employment while engaged in any activity that is a necessary incident to the rendition of his or her service or to the protection of the rights or property of the provider of that service, provided that a provider of wire or electronic communication service may not utilize service observing or random monitoring except for mechanical or service quality control checks.

(d) It is not unlawful under this Article for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of Chapter 5 of Title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(e) Any person who, as a result of the person's official position or employment, has obtained knowledge of the contents of any wire, oral, or electronic communication lawfully intercepted pursuant to an electronic surveillance order or of the pendency or existence of or implementation of an electronic surveillance order who shall knowingly and willfully disclose such information for the purpose of hindering or thwarting any investigation or prosecution relating to the subject matter of the electronic surveillance order, except as is necessary for the proper and lawful performance of the duties of his position or employment or as shall be required or allowed by law, shall be guilty of a Class G felony.

(f) Any person who shall, knowingly or with gross negligence, divulge the existence of or contents of any electronic surveillance order in a way likely to hinder or thwart any investigation or prosecution relating to the subject matter of the electronic surveillance order or anyone who shall, knowingly or with gross negligence, release the contents of any wire, oral, or electronic communication intercepted under an electronic surveillance order, except as is necessary for the proper and lawful performance of the duties of his position or employment or as is required or allowed by law, shall be guilty of a Class 1 misdemeanor.

(g) Any public officer who shall violate subsection (a) or (d) of this section or who shall knowingly violate subsection (e) of this section shall be removed from any public office he may hold and shall thereafter be ineligible to hold any public office, whether elective or appointed. (1995, c. 407, s. 1.)

§ 15A-288. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited.

(a) Except as otherwise specifically provided in this Article, a person is guilty of a Class H felony if the person:

- (1) Manufactures, assembles, possesses, purchases, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of the device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or
- (2) Places in any newspaper, magazine, handbill, or other publication, any advertisement of:
 - a. Any electronic, mechanical, or other device knowing or having reason to know that the design of the device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or
 - b. Any other electronic, mechanical, or other device where the advertisement promotes the use of the device for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(b) It is not unlawful under this section for the following persons to manufacture, assemble, possess, purchase, or sell any electronic, mechanical, or other device, knowing or having reason to know that the design of the device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications:

- (1) A communications common carrier or an officer, agent, or employee of, or a person under contract with, a communications common carrier, acting in the normal course of the communications common carrier's business, or
- (2) An officer, agent, or employee of, or a person under contract with, the State, acting in the course of the activities of the State, and with the written authorization of the Attorney General.

(c) An officer, agent, or employee of, or a person whose normal and customary business is to design, manufacture, assemble, advertise and sell electronic, mechanical and other devices primarily useful for the purpose of the surreptitious interceptions of wire, oral, or electronic communications, exclusively for and restricted to State and federal investigative or law enforcement agencies and departments. (1995, c. 407, s. 1.)

§ 15A-289. Confiscation of wire, oral, or electronic communication interception devices.

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of G.S. 15A-288 may be seized and forfeited to this State. (1995, c. 407, s. 1.)

§ 15A-290. Offenses for which orders for electronic surveillance may be granted.

(a) Orders authorizing or approving the interception of wire, oral, or electronic communications may be granted, subject to the provisions of this Article and Chapter 119 of the United States Code, when the interception:

- (1) May provide or has provided evidence of the commission of, or any conspiracy to commit:
 - a. Any of the drug-trafficking violations listed in G.S. 90-95(h); or
 - b. A continuing criminal enterprise in violation of G.S. 90-95.1.

- (2) May expedite the apprehension of persons indicted for the commission of, or any conspiracy to commit, an offense listed in subdivision (1) of this subsection.

(b) Orders authorizing or approving the interception of wire, oral, or electronic communications may be granted, subject to the provisions of this Article and Chapter 119 of the United States Code, when the interception may provide, or has provided, evidence of any offense that involves the commission of, or any conspiracy to commit, murder, kidnapping, hostage taking, robbery, extortion, bribery, rape, or any sexual offense, or when the interception may expedite the apprehension of persons indicted for the commission of these offenses.

(c) Orders authorizing or approving the interception of wire, oral, or electronic communications may be granted, subject to the provisions of this Article and Chapter 119 of the United States Code, when the interception may provide, or has provided, evidence of any of the following offenses, or any conspiracy to commit these offenses, or when the interception may expedite the apprehension of persons indicted for the commission of these offenses:

- (1) Any felony offense against a minor, including any violation of G.S. 14-27.31 (Sexual activity by a substitute parent or custodian), G.S. 14-27.32 (Sexual activity with a student), G.S. 14-41 (Abduction of children), G.S. 14-43.11 (Human trafficking), G.S. 14-43.12 (Involuntary servitude), G.S. 14-43.13 (Sexual servitude), G.S. 14-190.16 (First degree sexual exploitation of a minor), G.S. 14-190.17 (Second degree sexual exploitation of a minor), G.S. 14-202.1 (Taking indecent liberties with children), G.S. 14-205.2(c) or (d)(Patronizing a prostitute who is a minor or a mentally disabled person), or G.S. 14-205.3(b) (Promoting prostitution of a minor or a mentally disabled person).
- (2) Any felony obstruction of a criminal investigation, including any violation of G.S. 14-221.1 (Altering, destroying, or stealing evidence of criminal conduct).
- (3) Any felony offense involving interference with, or harassment or intimidation of, jurors or witnesses, including any violation of G.S. 14-225.2 or G.S. 14-226.
- (4) Any felony offense involving assault or threats against any executive or legislative officer in violation of Article 5A of Chapter 14 of the General Statutes or assault with a firearm or other deadly weapon upon governmental officers or employees in violation of G.S. 14-34.2.
- (5) Any offense involving the manufacture, assembly, possession, storage, transportation, sale, purchase, delivery, or acquisition of weapons of mass death or destruction in violation of G.S. 14-288.8 or the adulteration or misbranding of food, drugs, cosmetics, etc., with the intent to cause serious injury in violation of G.S. 14-34.4.

(d) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized, intercepts wire, electronic, or oral communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in G.S. 15A-294(a) and (b). Such contents and any evidence derived therefrom may be used in accordance with G.S. 15A-294(c) when authorized or approved by a judicial review panel where the panel finds, on subsequent application made as soon as practicable, that the

contents were otherwise intercepted in accordance with this Article or Chapter 119 of the United States Code.

(e) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this Article or Chapter 119 of the United States Code, shall lose its privileged character. (1995, c. 407, s. 1; 2013-368, s. 6; 2015-181, s. 46.)

§ 15A-291. Application for electronic surveillance order; judicial review panel.

(a) The Attorney General or the Attorney General's designee may, pursuant to the provisions of section 2516(2) of Chapter 119 of the United States Code, apply to a judicial review panel for an order authorizing or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offenses as to which the application is made, and for such offenses and causes as are enumerated in G.S. 15A-290. A judicial review panel shall be composed of such judges as may be assigned by the Chief Justice of the Supreme Court of North Carolina or an Associate Justice acting as the Chief Justice's designee, which shall review applications for electronic surveillance orders and may issue orders valid throughout the State authorizing such surveillance as provided by this Article, and which shall submit a report of its decision to the Chief Justice. A judicial review panel may be appointed by the Chief Justice or an Associate Justice acting as the Chief Justice's designee upon the notification of the Attorney General's Office of the intent to apply for an electronic surveillance order.

(b) A judicial review panel is hereby authorized to grant orders valid throughout the State for the interception of wire, oral, or electronic communications. Applications for such orders may be made by the Attorney General or the Attorney General's designee. The Attorney General or the Attorney General's designee in applying for such orders, and a judicial review panel in granting such orders, shall comply with all procedural requirements of section 2518 of Chapter 119 of the United States Code. The Attorney General or the Attorney General's designee may make emergency applications as provided by section 2518 of Chapter 119 of the United States Code. In applying section 2518 the word "judge" in that section shall be construed to refer to the judicial review panel, unless the context otherwise indicates. The judicial review panel may stipulate any special conditions it feels necessary to assure compliance with the terms of this act.

(c) No judge who sits as a member of a judicial review panel shall preside at any trial or proceeding resulting from or in any manner related to information gained pursuant to a lawful electronic surveillance order issued by that panel.

(d) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication must be made in writing upon oath or affirmation to the judicial review panel. Each application must include the following information:

- (1) The identity of the office requesting the application;
- (2) A full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including:
 - a. Details as to the particular offense that has been, or is being committed;
 - b. Except as provided in G.S. 15A-294(i), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted;

- c. A particular description of the type of communications sought to be intercepted; and
 - d. The identity of the person, if known, committing the offense and whose communications are to be intercepted;
- (3) A full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;
 - (4) A statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter must be added;
 - (5) A full and complete statement of the facts concerning all previous applications known to the individual authorizing and making adjudication, made to a judicial review panel for authorization to intercept, or for approval of interceptions of wire, oral, or electronic communications involving any of the same persons, facilities, or places specified in the application, and the action taken by that judicial review panel on each such application; and
 - (6) Where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(e) Before acting on the application, the judicial review panel may examine on oath the person requesting the application or any other person who may possess pertinent information, but information other than that contained in the affidavit may not be considered by the panel in determining whether probable cause exists for the issuance of the order unless the information is either recorded or contemporaneously summarized in the record or on the face of the order by the panel. (1995, c. 407, s. 1; 1997-435, s. 2; 2005-207, s. 1.)

§ 15A-292. Request for application for electronic surveillance order.

(a) The head of any municipal, county, or State law enforcement agency or any district attorney may submit a written request to the Attorney General that the Attorney General apply to a judicial review panel for an electronic surveillance order to be executed within the requesting agency's jurisdiction. The written requests shall be on a form approved by the Attorney General and shall provide sufficient information to form the basis for an application for an electronic surveillance order. The head of a law enforcement agency shall also submit a copy of the request to the district attorney, who shall review the request and forward it to the Attorney General along with any comments he may wish to include. The Attorney General is authorized to review the request and decide whether it is appropriate to submit an application to a judicial review panel for an electronic surveillance order. If a request for an application is deemed inappropriate, the Attorney General shall send a signed, written statement to the person submitting the request, and to the district attorney, summarizing the reasons for failing to make an application. If the Attorney General decides to submit an application to a judicial review panel, he shall so notify the requesting agency head, the district attorney, and the head of the local law enforcement agency which has the primary responsibility for enforcing the criminal laws in the location in which it is anticipated the majority of the surveillance will take place, if not the same as the

requesting agency head, unless the Attorney General has probable cause to believe that the latter notifications should substantially jeopardize the success of the surveillance or the investigation in general. If a judicial review panel grants an electronic surveillance order, a copy of such order shall be sent to the requesting agency head and the district attorney, and a summary of the order shall be sent to the head of the local law enforcement agency with primary responsibility for enforcing the criminal laws in the jurisdiction where the majority of the surveillance will take place, if not the same as the requesting agency head, unless the judicial review panel finds probable cause to believe that the latter notifications would substantially jeopardize the success of the surveillance or the investigation.

(b) This Article does not limit the authority of the Attorney General to apply for electronic surveillance orders independent of, or contrary to, the requests of law enforcement agency heads, nor does it limit the discretion of the Attorney General in determining whether an application is appropriate under any given circumstances.

(c) The Chief Justice of the North Carolina Supreme Court shall receive a report concerning each decision of a judicial review panel. (1995, c. 407, s. 1.)

§ 15A-293. Issuance of order for electronic surveillance; procedures for implementation.

(a) Upon application by the Attorney General pursuant to the procedures in G.S. 15A-291, a judicial review panel may enter an ex parte order, as requested or as modified, authorizing the interception of wire, oral, or electronic communications, if the panel determines on the basis of the facts submitted by the applicant that:

- (1) There is probable cause for belief that an individual is committing, has committed, or is about to commit an offense set out in G.S. 15A-290;
- (2) There is probable cause for belief that particular communications concerning that offense will be obtained through such interception;
- (3) Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and
- (4) Except as provided in G.S. 15A-294(i), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by the individual described in subdivision (1) of this subsection.

(b) Each order authorizing the interception of any wire, oral, or electronic communications must specify:

- (1) The identity of the person, if known, whose communications are to be intercepted;
- (2) The nature and location of the communications facilities as to which, or the place where, authority to intercept is granted, and the means by which such interceptions may be made;
- (3) A particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates;
- (4) The identity of the agency authorized to intercept the communications and of the person requesting the application; and

- (5) The period of time during which such interception is authorized, including a statement as to whether or not the interception automatically terminates when the described communication has been first obtained.

(c) No order entered under this Article may authorize the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than 30 days. Such 30-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or 10 days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with G.S. 15A-291 and the panel making the findings required by subsection (a) of this section. The period of extension shall be no longer than the panel determines to be necessary to achieve the purpose for which it was granted and in no event for longer than 30 days. Every order and extension thereof must contain a provision that the authorization to intercept be executed as soon as practicable, be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this Article, and terminate upon attainment of the authorized objective, or in any event in 30 days, as is appropriate. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after the interception. An interception under this Article may be conducted in whole or in part by State or federal government personnel, or by an individual operating under a contract with the State or federal government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(d) Whenever an order authorizing interception is entered pursuant to this Article, the order may require reports to be made to the issuing judicial review panel showing that progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports must be made at such intervals as the panel may require.

- (1) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this Article must be recorded on tape, wire, or electronic or other comparable device. The recording of the contents of any wire, electronic, or oral communication under this subsection must be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, the recordings must be made available to the judicial review panel and sealed under its direction. Custody of the recordings is wherever the panel orders. They may not be destroyed except upon an order of the issuing panel and in any event must be kept for 10 years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of G.S. 15A-294(a) and (b) for investigations. The contents of any wire, oral, or electronic communication or evidence derived therefrom may not be disclosed or used under G.S. 15A-294(c) unless they have been kept sealed.
- (2) Applications made and orders granted under this Article must be sealed by the panel. Custody of the applications and orders may be disclosed only upon a showing of good cause before the issuing panel and may not be destroyed except on its order and in any event must be kept for 10 years.
- (3) Any violation of the provisions of this subsection may be punished as for contempt.

(e) The State Bureau of Investigation shall own or control and may operate any equipment used to implement electronic surveillance orders issued by a judicial review panel and may operate or use, in implementing any electronic surveillance order, electronic surveillance equipment in which a local government or any of its agencies has a property interest.

(f) The Attorney General shall establish procedures for the use of electronic surveillance equipment in assisting local law enforcement agencies implementing electronic surveillance orders. The Attorney General shall supervise such assistance given to local law enforcement agencies and is authorized to conduct statewide training sessions for investigative and law enforcement officers regarding this Article. (1995, c. 407, s. 1; 1997-435, s. 2.1; 2005-207, ss. 2, 3.)

§ 15A-294. Authorization for disclosure and use of intercepted wire, oral, or electronic communications.

(a) Any investigative or law enforcement officer who, by any means authorized by this Article or Chapter 119 of the United States Code, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(b) Any investigative or law enforcement officer, who by any means authorized by this Article or Chapter 119 of the United States Code, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may use such contents to the extent such use is appropriate to the proper performance of the officers' official duties.

(c) Any person who has received, by any means authorized by this Article or Chapter 119 of the United States Code, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom, intercepted in accordance with the provisions of this Article, may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding in any court or before any grand jury in this State, or in any court of the United States or of any state, or in any federal or state grand jury proceeding.

(d) Within a reasonable time, but no later than 90 days after the filing of an application for an order or the termination of the period of an order or the extensions thereof, the issuing judicial review panel must cause to be served on the persons named in the order or the application and such other parties as the panel in its discretion may determine, an inventory that includes notice of:

- (1) The fact of the entry of the order or the application;
- (2) The date of the entry and the period of the authorized interception; and
- (3) The fact that during the period wire, oral, or electronic communications were or were not intercepted.

(d1) The notification required pursuant to G.S. 15A-294(d) may be delayed if the judicial review panel has probable cause to believe that notification would substantially jeopardize the success of an electronic surveillance or a criminal investigation. Delay of notification shall be only by order of the judicial review panel. The period of delay shall be designated by the judicial review panel and may be extended from time to time until the jeopardy to the electronic surveillance or the criminal investigation dissipates.

(e) The issuing judicial review panel, upon the filing of a motion, may in its discretion, make available to such person or his counsel for inspection, such portions of the intercepted communications, applications, and orders as the panel determines to be required by law or in the interest of justice.

(f) The contents of any intercepted wire, oral, or electronic communication, or evidence derived therefrom, may not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in any court of this State unless each party, not less than 20 working days before the trial, hearing, or other proceeding, has been furnished with a copy of the order and accompanying application, under which the interception was authorized.

(g) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of this State, or a political subdivision thereof, may move to suppress the contents of any intercepted wire, oral, or electronic communication, or evidence derived therefrom, on the grounds that:

- (1) The communication was unlawfully intercepted;
- (2) The order of authorization under which it was intercepted is insufficient on its face; or
- (3) The interception was not made in conformity with the order of authorization.

Such motion must be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of this motion. If the motion is granted, the contents of the intercepted wire, oral, or electronic communication, or evidence derived therefrom, must be treated as having been obtained in violation of this Article.

(h) In addition to any other right to appeal, the State may appeal:

- (1) From an order granting a motion to suppress made under subdivision (1) of this subsection, if the district attorney certifies to the judge granting the motion that the appeal is not taken for purposes of delay. The appeal must be taken within 30 days after the date the order of suppression was entered and must be prosecuted as are other interlocutory appeals; or
- (2) From an order denying an application for an order of authorization, and the appeal may be made ex parte and must be considered in camera and in preference to all other pending appeals.

(i) The requirements of G.S. 15A-293(b)(2) and G.S. 15A-293(a)(4) relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if:

- (1) In the case of an application with respect to the interception of an oral communication:
 - a. The application is by a State investigative or law enforcement officer and is approved by the Attorney General or his designee;
 - b. The application contains a full and complete statement as to why the specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and
 - c. The judicial review panel finds that the specification is not practical.
- (2) In the case of an application with respect to a wire or electronic communication:
 - a. The application is by a State investigative or law enforcement officer and is approved by the Attorney General or his designee;

- b. The application identifies the person believed to be committing the offense and whose communications are to be intercepted, and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;
- c. The judicial review panel finds that the showing has been adequately made; and
- d. The order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which the communication will be or was transmitted.

(j) An interception of a communication under an order with respect to which the requirements of G.S. 15A-293(b)(2) and G.S. 15A-293(a)(4) do not apply by reason of subdivision (i)(1) of this section shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subdivision (i)(2) of this section may move the court to modify or quash the order on the grounds that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously. (1995, c. 407, s. 1; 1997-435, s. 3; 2005-207, s. 4.)

§ 15A-295. Reports concerning intercepted wire, oral, or electronic communications.

In January of each year, the Attorney General of this State must report to the Administrative Office of the United States Court the information required to be filed by section 2519 of Title 18 of the United States Code, as heretofore or hereafter amended, and file a copy of the report with the Administrative Office of the Courts of North Carolina. (1995, c. 407, s. 1.)

§ 15A-296. Recovery of civil damages authorized.

(a) Any person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of this Article, has a civil cause of action against any person who intercepts, discloses, uses, or procures any other person to intercept, disclose, or use such communications, and is entitled to recover from any other person:

- (1) Actual damages, but not less than liquidated damages, computed at the rate of one hundred dollars (\$100.00) a day for each day of violation or one thousand dollars (\$1,000), whichever is higher;
- (2) Punitive damages; and
- (3) A reasonable attorneys' fee and other litigation costs reasonably incurred.

(b) Good faith reliance on a court order or on a representation made by the Attorney General or a district attorney is a complete defense to any civil or criminal action brought under this Article. (1995, c. 407, s. 1.)

§ 15A-297. Conformity to provisions of federal law.

It is the intent of this Article to conform the requirements of all interceptions of wire, oral, or electronic communications conducted by investigative or law enforcement officers in this State to provisions of Chapter 119 of the United States Code, except where the context indicates a

purpose to provide safeguards even more protective of individual privacy and constitutional rights. (1995, c. 407, s. 1.)

§ 15A-298. Subpoena authority.

The Director of the State Bureau of Investigation or the Director's designee may issue an administrative subpoena to a communications common carrier or an electronic communications service to compel production of business records if the records:

- (1) Disclose information concerning local or long-distance toll records or subscriber information; and
- (2) Are material to an active criminal investigation being conducted by the State Bureau of Investigation. (1995, c. 407, s. 1; 1997-435, s. 4; 2014-100, s. 17.1(ee); 2015-276, s. 4.)

Greater Cleveland Regional Transit Authority (RTA), Cleveland, Ohio

RTA Administrative Procedures, Security Camera Procedures

29



Greater Cleveland Regional Transit Authority
ADMINISTRATIVE PROCEDURES

Form 100-327
09-20-88
Rev. 07-17-02

TITLE SECURITY CAMERA PROCEDURES		NO. 55
		EFFECTIVE January 7, 2013
Prepared By Deputy General Manager – Operations	Issued By CEO, General Manager/Sec.-Treas.	

1.0 PURPOSE/OBJECTIVE

- 1.1 The Greater Regional Transit Authority holds the security and safety of employees, the riding public and others as its top priority. Security cameras are an important tool for keeping individuals and property as safe as possible.
- 1.2 The purpose of this document is to provide guidance regarding the use of security cameras at the Greater Cleveland Regional Transit Authority (GCRTA). Security cameras are used to enhance the security and safety of our customers, employees, and contractors and to facilitate more effective and efficient use of resources towards improving customer service.

2.0 REFERENCE

- 2.1 GCTRA System Security Plan.
- 2.2 Administrative Procedure No. 46 - Security Procedure for Vendors/Contractors and Subcontractors, Effective November 28, 2007.

3.0 DEFINITIONS

Fixed systems – Cameras and related hardware installed at fixed locations and interconnected via the GCRTA network.

Mobile systems – Cameras and related hardware systems that are aboard GCRTA revenue vehicles.

Police Mobile Systems – Cameras and related hardware systems that are aboard GCRTA police vehicles.

Active Monitoring – Camera video watched in real-time by an individual whose duties include monitoring security cameras.

Post Incident Documentation (PID) – Process where camera video is recorded and used after the incident.

Episodic Activation – Camera video automatically streamed to a monitor upon the activation of a specific trigger such as window breakage, ATM machine intrusion, Blue Light Telephone Call, etc. GCRTA generally utilizes the 'system' for Post Incident Documentation.

Pan-Tilt-Zoom (PTZ) – Security cameras featuring a motorized mount that allows the camera to be moved remotely up-down and side-to-side. In addition, the camera has a motorized zoom lens that can be moved in or out.

Digital Video Recorder (DVR) – The machine that records the video and audio signal.

4.0 GUIDELINES

Individual GCRTA managers are responsible for the proper and responsible monitoring practices of their employees:

- 4.1 Video monitoring for security, resource allocation and customer service purposes will be conducted in a professional, ethical, and legal manner. Monitoring individuals based on characteristics of race, gender, ethnicity, sexual orientation, disability, or other protected classifications is prohibited.
- 4.2 Information obtained through video monitoring will be used exclusively for law enforcement investigative purposes, safety, security, and operations.
- 4.3 Viewers will use discretion and not zoom in on any portion of a person other than for the purposes of determining an action taking place, identification, training, testing or equipment.
- 4.4 Viewers will not zoom cameras towards adjacent property unless a potential incident is in development and the Director of Security or his designee authorizes such camera control.

5.0 FIXED SYSTEMS

5.1 Responsibilities

- 5.1.1 The Security Systems Manager is responsible for the design, installation, maintenance and access to all fixed systems.
- 5.1.2 Access to the fixed system is made through the Security Systems Manager. The Security Systems Manager may grant access to one or all cameras. PTZ authorization will be granted on an as-needed basis. The Security Systems Technician will make the software available to the end user and to the Information Technology Department for loading to PCs. The end user is responsible for the maintenance of the software (updates and/or the adding of additional, authorized access).
- 5.1.3 In accordance with the Authority's desire to participate in regional collaboration, security camera systems may be shared with other organizations as part of Homeland Security Infrastructure protection and for general law enforcement purposes.

- 5.1.4 The Security Systems Technician will provide technical support for system training (Digital Sentry).
- 5.1.5 GCRTA employees requiring access to security camera images shall make their request known to the Security Systems Manager particularly requesting the camera access required and the business need for the access.
- 5.1.6 Each user account is the responsibility of the person issued the access. The system user is responsible for safeguarding their account and password

5.2 Fixed Video Retrieval

- 5.2.1 Requests for video on the fixed system will be made through one of the following utilizing the Video Request Form as soon as it is known that video is needed:
 - **Security Systems Manager, Specialist, or Technician**
 - **Transit Police** (Investigative Services) – criminal matters only
- 5.2.2 All search requests should be documented on a Video Request Form to include Incident data: (give date, time(s), agencies/individuals, and nature of incident) and reason for the request.
- 5.2.3 Each department is to budget and maintain PCs and related equipment capable of translating the captured video onto practicable media (CD/DVD/Network files, etc.)
- 5.2.4 The Information Technology Department is to budget for upgrade of drives, monitors and related systems that support the Fixed Security Camera System capturing terminals.
- 5.2.5 Video archive history on the fixed systems is subject to limitations of use and activity; capturing historic video is time critical.
- 5.2.6 The GCRTA unit that has removed video must notify the Police Dispatch Center at 216.566.5162 once any video media is removed, providing their name and where the media was removed. The Police Dispatcher will record the information in CrimeStar.

5.3 Fixed Video Viewing

- 5.3.1 The system is for GCRTA business or authorized law enforcement partners described in section 4.0; active viewing consumes network bandwidth, therefore video monitoring should only take place on a needed basis.
- 5.3.2 Reviewing video history consumes vast network resources and should be limited on an as needed basis.

5.5 Fixed Video Maintenance

Users should report security camera system problems or service requirements to the Transit Police Dispatch Center (216.566.5162).

5.6 Historic Fixed Video

All retained, streamed video must be transferred to a CD or other removable media in the proprietary format suitable for post-incident review. If there is a need for post incident documentation of an incident, that the search for the video be made as soon after the incident as possible due to varying archive limitations and potential equipment failures.

5.7 Non-Users

Non-users can request to view or obtain a copy of an incident by contacting Transit Police Dispatch (216.566.5162).

5.8 Users Without Removable Media Recording Capability

The Security Technician will burn video stream in the proprietary format on a periodic basis, if a user has need for PID:

5.8.1 Outside requests for video stream shall be referred to the Legal Department.

5.8.2 Law Enforcement agency requests should be referred to the Director of Security or his designee.

6.0 MOBILE SYSTEMS

6.1 Responsibilities

6.1.1 Security Systems Manager and Fleet Management are responsible for the design, installation, maintenance and access to all mobile systems.

6.1.2 Fleet Management will train operators on their daily review of the system.

6.1.3 Para-transit and Bus Operators are responsible for inspecting their coach prior to pullout. If the video status light indicates a defect, the operator shall note that indication on the Pre-Trip Inspection and Defect Card, Form 72-628, prior to pullout.

6.1.4 Rail Operators are responsible for inspecting their coach prior to pullout. If the video status light indicates a defect, the operator shall note that indication during the Pre-Trip Inspection.

6.1.5 Each Bus and Rail Operator is responsible to push the "Event" button when required.

6.1.6 Hostlers are to check the video status light indicator at time of fueling and shall note any problems on the Pre-Trip Inspection and Defect Card.

- 6.1.7 The Transit Police Department is responsible for all mechanical and electronic locks associated with the DVR box. The Security Technician will issue keys utilizing the Electronic Key Watcher boxes assigned to each District.

6.1.8 Pre-Trip Inspections When Trains Made Up and Prior to Pullout

Rail Operators and Yard Persons will be responsible for ensuring that all on-board camera systems and monitors are in working order as trains are made up for daily pullout. (This includes replacement cars or trains or additional cars or trains added to service during the service day.) Confirmation of this equipment's working order must be made by radio to the ICC Yard Control Supervisor and/or Control Center Supervisor at the time the train is made up.

Rail Operators will be responsible for ensuring that all on-board cameras and monitors are in service before their train pulls out of the yard to enter revenue service.

Inspection of this equipment by Rail Operators will be in accordance with the requirements of the Rail Operator Pre-Trip Report Form 72-1257. Inspection results must be recorded on this form in the designated space(s) with comments added by the Rail Operator when required.

Any equipment found defective must be immediately reported by radio to the ICC Yard Control Supervisor, Security Systems Specialist and Control Center Supervisor.

The Control Center Supervisor shall make arrangements as required for repairs to equipment or for replacement of the train. NB: Multiple Car Light Rail Trains will not be permitted to enter service without fully operable cameras and monitors.

6.1.9 Defective Equipment When Trains are in Revenue Service

Any camera or monitoring equipment that becomes defective when a train is in revenue service must be immediately reported by radio by the Rail Operator to the ICC Control Center Supervisor.

The Control Center Supervisor shall record the information and immediately provide the defect information to the Load Dispatcher. The Load Dispatcher shall enter this information as a "Work Request" in the Ultramain CITME Program and send the Work Request to the Supervisor Electronic Repair, Fleet Management District and the Rail Equipment Manager, Rail District.

The Control Center Supervisor shall make arrangements as required for in or out-of-service repairs to equipment and/or for replacement of the train. NB: Multiple Car Light Rail Trains will not be permitted to operate as multiple car trains without fully-operable cameras and monitors. A qualified staff person may be used as a car monitor in the trailing car(s) until the defective car or train can be replaced, and/or the trailing car (or cars) may be put out of service and the train operated as a single car train using only the lead car.

Rail Operators and Yard Persons will be responsible for ensuring that all on board camera systems and monitors are in working order as trains are made up for daily pullout. (This includes replacement cars or trains or additional cars or trains added to service during the service day.) Confirmation of this equipments' working order must be made by radio to the ICC Yard Control Supervisor and/or Control Center Supervisor at the time the train is made up.

6.2 Mobile Video Retrieval

6.2.1 Requests for video on the mobile system will be made through one of the following utilizing the Video Request Form as soon as it is known that video is needed:

- **Security Systems Manager, Specialist, or Technician** (Internal Request)
- **Transit Police** (Investigative Services) – criminal matters only
- **Service Quality Management /Safety-** Safety related incidents
- **Claims** - Claim for an injury

6.2.2 All search requests should be documented on a Video Request Form (VRF) to include Incident data: (give date, time(s), agencies/individuals, and nature of incident), reason for the request, the coach/train number and location of coach train at the time of the incident.

6.2.3 Each department is to budget and maintain PCs and related equipment capable of translating the captured video onto practicable media (CD/DVD/Network files, etc.).

6.2.4 The Fleet Management is to budget for upgrade of drives, monitors and related systems that support the Mobile Security Camera System capturing terminals.

6.2.5 Video archive history on the mobile systems is subject to limitations of vehicle use and activity; capturing historic from the coach or train is time critical.

6.2.6 The GCRTA unit that has removed video must notify the Police Dispatch Center at 216.566.5162 once any video media is removed, provide their name and the coach / train from which the media was removed. The Police Dispatcher will record the information in CrimeStar.

6.3 Historic Mobile Video

All retained, streamed video must be transferred to a CD or other removable media in the proprietary format suitable for post-incident review. If there is a need for post incident documentation of an incident, that the search for the video be made as soon after the incident as possible due to varying archive limitations and potential equipment failures.

6.4 Non-Users

Non-users view or obtain a copy of an incident by contacting the appropriate department listed above.

6.5 Users Without Removable Media Recording Capability

The Security Systems Specialist will burn video stream on an as needed basis.

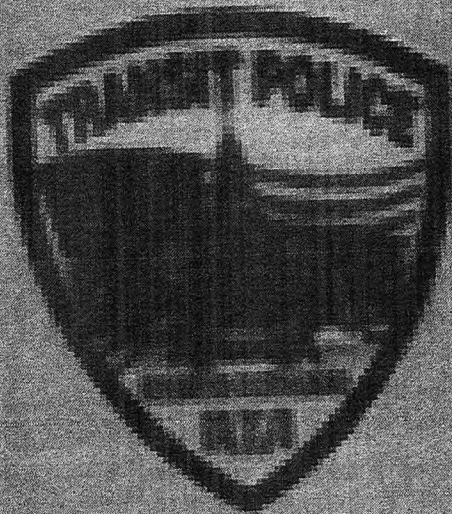
- All outside requests for video stream shall be referred to the Legal Department.
- Law Enforcement agency requests should be referred to the Director of Security or his designee.

7.0 PROHIBITIONS

- 7.1 Disabling or tampering with any GCRTA security-monitoring device, including security camera equipment.
- 7.2 Unauthorized access or use of security camera software or systems.
- 7.3 Physically relocating or re-positioning a fixed-lens camera.
- 7.4 Covering or otherwise obstructing the lens of any camera.
- 7.5 Installation or use of security cameras or any type video-captured equipment not pre-approved by the Director of Security or Security Systems Manager.
- 7.6 Authorizing or utilizing non-security systems staff for any type of service related to security cameras, equipment or systems.

8.0 RESPONSIBILITY

- 8.1 It is the responsibility of all Authority employees to maintain all camera/video documents in compliance with the GCRTA Records Retention Schedule.
- 8.2 It is the responsibility of all Authority employees to comply with this administrative procedure as may be applicable.



**This Location Is Under
24 Hour
Electronic Surveillance
RTA Transit Police 216-566-5153**

NOTICE
THIS VEHICLE IS UNDER
ELECTRONIC SURVEILLANCE

- 209.3 The BLUE lights are status lights. They are always "ON" if the system is operational.
- 209.4 AMBER lights
- A. Flashing Slowly -- object is within the FAR (4 feet) zone.
 - B. Flashing Fast -- object is within the MID (3 feet) zone.
 - C. Solid -- object is within the NEAR (2 feet) zone. You have very little maneuvering room with your mirror and bumper overhang.
- 209.5 Urban Fast Mode
- A. 25 mph, the ODS is TURN SIGNAL activated.
 - B. An audible signal and SOLID AMBER lights are activated when the bus cannot safely move more than ½ a lane in that direction.
- 209.6 Highway Mode
- A. 55 mph
 - B. Audible signal and SOLID AMBER lights when the turn signal is activated and a lane change would be unsafe with objects adjacent to the vehicle.
- 209.7 If another vehicle is approaching 25 to 20 MPH faster than your speed, the system might not detect the approaching vehicle.

210 Cameras

- 210.1 Coaches are equipped with interior and exterior video cameras. The cameras are continuously recording. The recordings are reviewed during investigations of accidents, passenger accident claims, customer service issues, and crimes.
- 210.2 Monitor camera status lights and report malfunctions to Service Quality and make a notation on the defect card.
- 210.3 Press the incident button (flat round green button) whenever you are involved in an accident, advised of a passenger accident, or are involved in a customer dispute.

Greater Peoria Mass Transit District, Peoria, Illinois

Surveillance Camera Policy

32

SURVEILLANCE CAMERA POLICY

PURPOSE

The purpose of the surveillance cameras on all facilities and vehicles is to provide a mechanism to record activity which has the potential for adverse effects against the District. The surveillance cameras may be used as part of the operational duties to conduct accident/incident investigations, complaints and audits with the primary goal of ensuring safe transportation for all employees and passengers.

The images from the surveillance cameras will not be continuously monitored. The images will be stored and kept for the purpose of review in the event that a problem is brought to the attention of the appropriate departmental staff. Only those responsible for the system administration of the security system will have access to the stored images. The retention of images collected will typically be 30 days.

VEHICLE CAMERAS

All revenue generating vehicles to include supervisory vehicles will be equipped with surveillance cameras. The information below will be used as a baseline for camera installation:

30' 35', 40' coaches and trolley's

Camera 1 will be mounted in the front of the coach with a street facing view.

Camera 2 will be mounted above the driver's station with a view of the front door and fare box.

Camera 3 will be mounted adjacent to the rear door with a view of the entire entrance (*Except trolley's*).

Camera 4 and 5 will be mounted to ensure views both frontal and rear views of the interior of the coach.

Camera 6 will be mounted on the right side exterior of the coach viewing the rear entrance door (*Except trolley's*).

Event trigger switch with status lights will be placed in the driver's compartment within the operators reaching distance.

Supervision vehicles

Camera will be mounted in the front of the vehicle with a street facing view.

Event trigger switch with status lights will be placed within the operators reaching distance.

FACILITY CAMERAS

Cameras will be positioned to provide 360 degrees of coverage throughout the Administration and Transit Center facilities.

POSTING

Public notification shall be posted on all vehicles and facilities with video surveillance in use.

ACCESS

All access to video data must be authorized (See Attachment A). Access will be provided whenever required by law or a court order. The General Manager must authorize all requests submitted for video data access. The completed request form must then be presented to the system administrator. No other use will be made of the images without the appropriate management approval. Access to the stored data will be through the appropriate system administrator. The system administrator will maintain a log of all access to data and/or DVR removal.

MAINTENANCE OF CAMERAS

To ensure that the surveillance system is maintained, the Maintenance Department will schedule periodic services on all components of the surveillance system which includes but not limited to:

- Cleaning of all camera dome lenses
- Secure mounting of all cameras and components
- Chaffing and looseness of all wiring
- Cleaning of DVR box and router interface
- Proper public notice is posted

On a semi-annual basis the system administrator will complete a function test of the surveillance system to ensure all equipment is in proper working order. This will include, but not limited to:

- Testing the system internal clock and date
- Ensuring proper camera focus and viewing area
- Testing the internal wireless router
- Removal of outdated video segments

No components of the system will be removed or replaced without prior approval from the system administrator. All preventative and scheduled maintenance performed will be logged and maintained on file.

Attachment A

**Greater Peoria Mass Transit District
Request for Review of Video**

Date: _____

Party Requesting to View Data: _____

Bus Number Requested: _____ Operator: _____

Date Of Event: _____ Time Of Event: _____ Route #: _____

INC/ACC#: _____

Purpose for Request: _____

The party requesting to view the data represents that its review is solely for the purposes listed above, and further agrees that he/she will not make any disclosure of the contents of the tape for purposes other than as described, without prior notification to Greater Peoria Mass Transit District.

Date: _____

Signature: _____

Agency: _____

Authorized by: _____

Hillsborough Transit Authority (HART), Tampa, Florida

Standard Operating Procedure, Video/Audio Surveillance Procedures

34

SOP NUMBER	REVISION	EFFECTIVE DATE	PAGE
SAFSOP-0005	04	November 30, 2009	1 of 11

STANDARD OPERATING PROCEDURE

HILLSBOROUGH TRANSIT AUTHORITY

VIDEO/ AUDIO SURVEILLANCE PROCEDURES

REV #	DATE	DESCRIPTION	INIT
00	11/2009	CREATED	JD
01	1/2011	ANNUAL REVIEW	DK
02	8/2012	ANNUAL REVIEW	DK
03	10/2013	ANNUAL REVIEW	DK
04	2/2016	ANNUAL REVIEW	DK

Originated By: _____
David Kelsey, Manager of Safety and Security _____ Date

Reviewed By: _____
Rickey Kendall, Director of Risk _____ Date
Management Safety

Reviewed By: _____
Dara Chenevert, Interim Chief Business _____ Date
Enterprise & Safety Officer

Approved By: _____
Katharine Eagan, AICP _____ Date
Chief Executive Officer

SOP NUMBER	REVISION	EFFECTIVE DATE	PAGE
SAFSOP-0005	03	November 30, 2009	2 of 11

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
1. SCOPE.....	3
2. PURPOSE.....	3
3. ABBREVIATIONS / DEFINITIONS	3
4. REFERENCES.....	4
5. FORMS	4
6. REQUIRED SAFETY EQUIPMENT/SPECIAL TOOLS	4
7. PROCEDURES.....	4
APPENDIX A – VIDEO/AUDIO SURVEILLANCE RECEIPT	11

SOP NUMBER	REVISION	EFFECTIVE DATE	PAGE
SAFSOP-0005	03	November 30, 2009	3 of 11

1. SCOPE

This SOP establishes the guiding principles relative to surveillance, monitoring, video surveillance and audio recording devices installed on board HART vehicles and at HART facilities, including hand held surveillance and recording devices. This surveillance procedure is managed under and as part of the Risk Management Program pursuant to Florida Statutes, Section 768.28.

2. PURPOSE

The SOP provides information to HART employees, customers, and the general public on how HART communicates where and how video and audio surveillance recording equipment will be used; the process for internal and external requests for copies of recordings; the internal processes and procedures in place for ensuring that the chain of custody retrieval of recordings is controlled and protected; and, record retention.

3. ABBREVIATIONS / DEFINITIONS

ABBREVIATIONS	DEFINITIONS
FS	Florida Statutes
SOP	Standard Operating Procedure
HART	Hillsborough Transit Authority
Digital Video Monitoring System	Videos or other equipment used for vehicle, personal, and building security systems for VCR, DVR, or personal computer.
Electronic Surveillance System	System used to protect persons and infrastructure from break-ins, burglary, theft, robbery, and assault, or other criminal activity as part of the risk management program. These systems can be in the form of burglar alarms that notify the police, security cameras, handheld devices, and closed circuit television systems.
Video Surveillance System	Electronic system used to ensure the safety and security of the vehicle, building and its occupants and risk matters. This system can be in the form of burglar alarms, analog cameras that notify the central station, security cameras, and closed circuit television systems.
Audio Surveillance System	Monitors or conducts surveillance in the form of an audio type device or equipment.
CD/DVD	Compact disc/digital video device
PR#	Payroll Number
PRR	Public Records Request Office

SOP NUMBER	REVISION	EFFECTIVE DATE	PAGE
SAFSOP-0005	03	November 30, 2009	4 of 11

4. REFERENCES

Florida Statutes Chapters 768 and 119

5. FORMS

Attachment A – Video/Audio Surveillance Receipt Form

6. REQUIRED SAFETY EQUIPMENT/SPECIAL TOOLS

Authority will provide.

7. PROCEDURES

A. Internal HART Department Request for Surveillance Video

1. All requests for surveillance video/audio will be made to the HART Risk Management Department and HART Safety and Security Department via e-mail. The request should include as much information as possible, i.e. date, time, location, direction of travel, facility, location, vehicle number, route number, employee name and PR# (if HART employee is involved), description of incident and description of any other external vehicles, persons, etc.
2. HART Risk Management in conjunction with HART Safety and Security personnel will schedule retrieval of surveillance video. If request is for video from a HART vehicle, schedule for retrieval must also be coordinated through HART Dispatch and/or Maintenance Department.
3. If applicable, time and cost involved in researching, retrieving, downloading, recording and burning video to CD/DVD will be tracked, forwarded, and allocated to the department making the request. HART department head will receive a copy of the HART video/audio surveillance receipt form providing detail of time, cost, and process.
4. If requested to burn video to CD/DVD, HART Risk Management must provide signature authorization on HART's Chain-of-Custody Form prior to CD/DVD being made available to HART department/personnel.

B. External Agency / HART Employee/Public / HART Bargaining Units Request for Surveillance Video

1. All video and audio recordings are considered part of the Risk Management Program and considered Risk Files and Records under FS, Section 768.28 and will be considered exempt from disclosure until a full investigation of the situation is completed.

SOP NUMBER	REVISION	EFFECTIVE DATE	PAGE
SAFSOP-0005	03	November 30, 2009	5 of 11

2. All public requests for surveillance video/audio records will be forwarded to the HART PRR. Requests will follow established procedures for Public Record Requests. The PRR Staff will immediately notify Risk and Safety and Security of all requests.
 - a. The HART PRR staff will forward all requests via e-mail to HART Risk Management Department for approval.
 - b. HART's Risk Management Department will review and determine if the request is exempt under the Risk Management Program and FS, Section 768.28. Risk Management will forward an e-mail request back to PRR staff and copy the Safety and Security Department should the request be denied pursuant to the Risk Management Program and FS, Section 768.28. There may be other exemptions that may apply and such will be noted by PRR.
 - c. HART's Risk Management Department will forward e-mail request to the Safety and Security Department and copy HR should request be approved.
3. The request should include as much information as possible, i.e. date, time, location, direction of travel, facility, vehicle number, route number, employee name and PR# (if HART employee involved), description of incident and description of any other external vehicles, persons, etc.
4. Safety and Security Department personnel in conjunction with the Risk Department will schedule retrieval of surveillance video (audio); if request is for video from a HART vehicle, schedule for retrieval must also be coordinated through HART Dispatch and/or Maintenance Department.
5. If applicable, time and cost involved in researching, retrieving, downloading, recording and burning video to CD/DVD will be tracked, forwarded, and allocated to the requesting party pursuant to FS Chapter 119 and HART policy if the request is not exempt.
 - a. Copy of the HART Video/audio surveillance receipt form providing detail of time, cost, and process will be provided.
 - b. Payment for public records requests will be collected by the Public Records Office.
6. If requested to copy video/audio to CD/DVD, HART Risk Management must provide signature authorization on Video Receipt Form prior to CD/DVD being made available and only if the information is determined by Risk Management not to be exempt under or pursuant to FS, Section 768.28, the Risk Management Program or other Florida Statutes or laws.
7. The use of thumb drives/memory sticks is authorized as a means of transferring video to any requester. The same processes using CD/DVD technology will be used.

SOP NUMBER	REVISION	EFFECTIVE DATE	PAGE
SAFSOP-0005	03	November 30, 2009	6 of 11

C. General Process

1. Pursuant to the Risk Management Program and in conjunction with the Risk Department, only trained and authorized HART System Safety and Security personnel are authorized to retrieve, download, record, and burn video/audio.
2. All external and internal requests for video/audio will be logged by the Risk Department in conjunction with HART System Safety and Security personnel.
3. Only in extreme emergency situations will requests for surveillance video be performed immediately/at time of incident; coordination between Risk Management and Safety and Security must still take place. Risk Management along with Safety and Security shall determine what constitutes an extreme emergency.
4. Extreme care must be given with surveillance that involves exempted information and disclosure of certain individual identities as provided in FS, Section 768.28, the Risk Management Program and FS, Chapter 119.
5. Requests by law enforcement for surveillance video/audio will be given priority and such requests will be provided pursuant to the Public Record Exemption to another government agency and will be labeled accordingly. However, should the request/event occur after normal business hours, or should the event/request be made for video from an in-service bus and the event giving rise to the request is not an extreme emergency, then all pertinent information pertaining to the event will be recorded through HART standard established reporting procedures by the on-duty Dispatcher and/or the on-scene Transit Supervisor and forwarded to Risk Management and Safety and Security.
 - a. Dispatcher or Transit Supervisor will notify Risk Management and Safety and Security of law enforcement requests via e-mail.
 - b. Risk Management, in conjunction with Safety and Security personnel will contact the investigating law enforcement personnel next business day.
 - c. Established interdepartmental coordination process described above will be followed.

D. Retention and Disposal

1. The Risk Management Department under the Risk Management Program and the Safety and Security Department shall ensure that proper procedures are followed regarding disclosure, retention, disposal and security of video and audio surveillance records in accordance with applicable laws and regulations.
2. All video/audio records or surveillance equipment not in use shall be stored in a secured location.

SOP NUMBER	REVISION	EFFECTIVE DATE	PAGE
SAFSOP-0005	03	November 30, 2009	7 of 11

3. All video/audio records that have not been viewed shall be disposed of after thirty (30) days.
4. Any video/audio records that have been viewed will be stored noting the dates, times, and areas that were recorded.
5. When recorded information has been viewed for law enforcement, or public safety purposes, the information must be retained and securely stored for a minimum of one year or as provided under Florida Statutes unless the Risk Management Department or Florida Statutes allows for and determines that earlier disposal is warranted and the individual to whom the information relates consents to earlier disposal. (Note: Florida Statutes, the Risk Management Program and other court rules provide that some records cannot be deleted until a court releases it.)
6. The Risk Management Department and the Safety and Security Department will be responsible for ensuring the proper retention of records. Records will be disposed of in a manner such that personal or other required information cannot be reconstructed or retrieved and as provided via Florida Statutes.

E. Security Monitoring

1. Monitors for 'real time' viewing of video/audio surveillance will be placed in an area out of view from the public.
2. Monitors shall only be viewed by authorized or designated HART staff.
3. Video/audio surveillance information shall only be viewed and monitored where an incident has been reported or observed, or to investigate a potential crime or violation of HART rules.
4. The Risk Department and the Safety and Security Department will be responsible for securing video/audio surveillance information against tampering and ensuring confidentiality in accordance with applicable laws and regulations.

F. Purchase, Installation and Maintenance of Surveillance Camera and Equipment

1. All video / audio / electronic surveillance cameras, equipment, recordings, and images that are electronically and digitally stored on computers and hard copies are considered property of HART and are under the Risk Management Program, are considered Risk Management records and files and part of the Risk Management Program and are subject to the rules, policies, and regulations set by HART Risk Management Program and the HART Board of Directors as well as meeting the statutory standards established by local, state, and federal laws.

SOP NUMBER	REVISION	EFFECTIVE DATE	PAGE
SAFSOP-0005	03	November 30, 2009	8 of 11

2. All video / audio / electronic surveillance equipment must be purchased through approved HART vendors based upon the specific guidelines and specifications set forth in the bids and contracts as developed by HART. The installation and maintenance of all surveillance equipment must be completed under the direction and supervision of the Risk Management Program and HART designated departments / personnel to ensure that all building code and safety standards are met.

G. Authorization, Access and Use of Video Cameras and Related Equipment

1. Only HART trained and authorized personnel shall have access to operating, monitoring, and retrieving data from security cameras. Unauthorized use, monitoring, surveillance, or misuse of any surveillance equipment or disabling or tampering with video cameras or related equipment by unauthorized persons/employees will result in the appropriate corrective/disciplinary action as covered by state law and/or HART procedures, up to and including termination.
2. The use, by way of monitoring, viewing, printing, and copying any images from any and all HART surveillance equipment is under the direct control of the Risk Management Department and the Safety and Security Department. The Director of Risk and Safety and the Manager of Safety and Security have ultimate responsibility to ensure that the video equipment and the use, storage, and release of any information or images are in keeping with procedures and guidelines established within this document.
3. The Risk Management Department in conjunction with Safety and Security shall maintain a master list of those HART individuals who have been authorized and trained to use, view, retrieve, or copy images or data from video surveillance equipment. The authorization of such privileges will be restricted to the fewest number of staff as practical.
4. The Director of Risk and Safety and the Manager of Safety and Security will ensure that authorized HART personnel receive operational training of the equipment and that they practice fair and ethical use of the surveillance equipment including an annual training, which includes a review of equipment use/maintenance, and all privacy measures. Documentation of such training is to be used to show that such training has been provided. This training will also review the restrictions and exemptions under FS, Section 768.28 and public record exemption that apply under FS, Chapter 119.
5. Care and caution shall be taken by all HART personnel authorized to view, monitor, print, or access images and information from surveillance equipment to ensure that privacy rights are protected

SOP NUMBER	REVISION	EFFECTIVE DATE	PAGE
SAFSOP-0005	03	November 30, 2009	9 of 11

as required by HART guidelines, the Risk Management Program requirements and all local, state, and federal statutes.

H. Video/Audio Surveillance Primary Purpose

1. The use of surveillance equipment primarily serves as a Risk Management resource under the Risk Management Program and also a safety and security tool to protect HART employees, customers and assets. It also serves as a deterrent to inappropriate behaviors or the intrusion of trespassers within the HART system. It is the responsibility of HART to conduct any and all investigations, and to use all resources and investigative tools available, including radio, audio and telephone recordings, GPS, written reports, photographs, diagrams, courtesy cards, interviews, and video surveillance at HART facilities and on vehicles to assist in the investigation of accidents, incidents, customer service reports, etc.
2. HART does not randomly monitor video/audio surveillance for the purpose of administering discipline to employees; however, in the process of review, when investigating claims of accident, complaint, incident, or customer service reports, should there be a discovery of breach of standard operating procedures, policies and/or contractual obligations, appropriate corrective action (counseling, retraining, discussion log, etc.) will be taken to address the issue, up to and including termination.

I. Other Considerations

1. Camera (video equipment) locations will be identified by authorized HART management personnel.
2. Cameras will be installed in areas where there is a need for surveillance (i.e. vehicles, hallways, stairwells, entryways, outside areas, and other areas open to public view) as determined by management personnel.
3. Cameras will be installed in such a way that only the identified area(s) will be monitored.
4. Video surveillance cameras will not monitor the insides of lavatories or locker rooms.
5. HART's Risk Department under and as part of the Risk Management Program in conjunction with the Safety and Security Department shall maintain control of and responsibility for the video/audio surveillance system at all times.
6. Any agreements between HART and service providers will state that records dealt with or created while delivering a video surveillance system are under HART control and are subject to this procedure.

SOP NUMBER	REVISION	EFFECTIVE DATE	PAGE
SAFSOP-0005	03	November 30, 2009	10 of 11

7. If a service provider fails to abide by this Procedure, it will be considered a material breach of contract and dealt with accordingly.
 8. Individuals who deliberately breach this Procedure will be subject to the appropriate corrective action as applicable up to and including termination/contract termination or other legal remedies.
- J. HART will notify employees, customers, and the general public of the existence of video surveillance systems. Such notice will be included in various HART publications as well as appropriate signage posted at facilities and on-board vehicles. Audio and radio monitoring will be noticed as required by law, if any.

SOP NUMBER	REVISION	EFFECTIVE DATE	PAGE
SAFSOP-0005	03	November 30, 2009	11 of 11

APPENDIX A – VIDEO/AUDIO SURVEILLANCE RECEIPT



HILLSBOROUGH TRANSIT AUTHORITY

RISK MANAGEMENT PROGRAM

RISK MANAGEMENT DEPARTMENT AND OFFICE OF SAFETY AND SECURITY

VIDEO/AUDIO SURVEILLANCE RECEIPT FORM

Person/Department/Agency Requesting Video: _____

Mailing Address: _____

Phone #: _____

Reason for Request _____

Vehicle # / Facility of Event _____

Time of Event: _____ Date of Event: _____

ID. /Log #: _____ Date of Recovery: _____ Time of Recovery: _____

Name of Collector (print): _____ PR#: _____

Explanation if Unable to Recover: _____

Time Involved Recovering: _____ Cost per/hour _____ Total: _____

Identify All Additional Material: _____

Material Cost: _____

Total Cost Due: _____

Signature of Collector: _____ Date _____

Relinquished by (signature): _____ Date/Time: _____

Received by (signature): _____ Date/Time: _____

Risk Department Authorization to Release (signature): _____

Time: _____ Date: _____

ATTENTION

This Unit is
equipped with

video and audio
monitoring
equipment.

 **HART**

HART is a registered trademark of HART Corporation.

Intercity Transit, Olympia, Washington

Intercity Transit Policy-OP-5507, Managing Digital Video Recording
System

37

Effective: June 7, 2007
Cancels: New

Page: 1 of 2

INTERCITY TRANSIT POLICY-OP-5507

See Also: PR-OP-5507-A, Retrieving DVR Hard Drives; PR-OP-5507-B, Auditing Monthly DMERS

Approved by: 

TJ Johnson, Chair
Intercity Transit Authority


Michael Harbour, General Manager

Written by: Jim Merrill

Managing Digital Video Recording System.

Definitions:

"DVR System" — a digital video recorder, microphone and cameras installed in all Intercity Transit revenue vehicles. The system records digital video images in all sections of the interior of the vehicle and audio in the fare box area. The system also records digital video images of the front exterior and curb side exterior of the vehicles.

This policy applies to all Intercity Transit staff responsible for management of the "DVR system" and those employees with access to the DVR system.

1. Equipment and Use Comply With Laws and Regulations

The equipment and its use shall comply with all pertinent federal, state and local laws or regulations. Staff will post notices in buses and on the outside of buses where recording equipment is installed. When staff saves a recording, they will retain the material in a confidential manner. Law enforcement and/or legal counsel may consider recordings evidence. Staff will disclose recordings to the public upon request, when the recordings are subject to disclosure and the request meets public disclosure rules.

2. DVR System Recordings Considered Confidential

Staff considers all materials generated by the DVR system as confidential. Staff will review materials under certain situations, such as, but not limited to:

- Accidents
- Incidents
- Investigations of misconduct
- Operator requests
- Passenger complaints
- Processing a public records request
- Police requests

INTERCITY TRANSIT POLICY-OP-5507

3. Staff Shall Handle Materials Appropriately

The General Manager or designee establishes procedures to limit staff review of the DVR system materials and to ensure staff handles DVR system materials in an appropriate manner. The procedures include staff documenting when, by whom and the circumstances under which staff shall review materials.

Documentation will include any decision to retain or not to retain reviewed material, why that decision was made and by whom. The procedures will track when and why staff made copies of any saved material and who authorized the duplication.

Staff will include in the procedures a prohibition on any unauthorized use of the system or any materials the system generates. The procedure includes an illustration of the consequences of any violation of the respective procedures.

4. Willful Policy Violation Results In Serious Discipline

The General Manager or designee will ensure any willful violation of Policy-OP-5507 will result in serious discipline, up to and including termination of employment.

INTERCITY TRANSIT PROCEDURE-OP-5507-A

See Also: Policy-OP-5507, Managing Digital Video Recording System; Procedure-OP-5507-B, Auditing Monthly DMERS

Approved by: 
Director of Operations

Written by: Jim Merrill

RETRIEVING DVR HARDDRIVES

Definitions:

"Incident" – accidents, customer complaints and security incidents that could focus public attention on the agency, create a financial or legal obligation, or involve a violation of Intercity Transit rules or regulations. Accidents include events involving damage to a vehicle and/or injuries. Customer complaints include those requiring an investigation and/or where there is disagreement on what actually occurred. Security incidents include crimes, arrests on Intercity Transit property, vandalism damage, altercations, display of weapons, threatening behavior, violations of Intercity Transit's Rules of Conduct or other incidents that might generate media coverage or create a financial or legal exposure for Intercity Transit.

"DVRs" – digital video recording system.

"DMER" – digital master evidence record form.

Action By:

Fixed Route
Manager

Action:

1. **Receives** notification of an "incident" on a transit revenue vehicle.

2. **Decides** an investigation is required.

3. **Sends** written instructions, a "DVRs" Master Evidence Record form (FORM-OP-5507), and a replacement Digital Video Recorder (DVR) hard drive to an Operations Supervisor.

Operations
Supervisor

4. **Retrieves** DVR hard drive as directed, **replaces** hard drive with spare, and **fills** out a "DMER" as required.

5. **Submits** the DMER and hard drive to Fixed Route Manager.

Fixed Route
Manager

6. **Reviews** materials.

6a. If material deemed important, **makes** copy and **places** in secured cabinet. (TASK-OP-5507-A)

INTERCITY TRANSIT PROCEDURE-OP-5507-A

6b. If **determines** material unimportant, **skips** to step 7.

7. **Determines** the DVR hard drive may be returned to its assigned vehicle.
8. **Sends** written instruction, DMER for completion, and original hard drive to Operations Supervisor.

Operations
Supervisor

9. **Returns** DVR hard drive to vehicle.
10. **Completes** DMER and **returns** the form and spare hard drive to Fixed Route Manager.

Fixed Route
Manager

11. **Places** DMER in a designated secured cabinet.

INTERCITY TRANSIT PROCEDURE-OP-5507-B

See Also: Policy-OP-5507-Managing Digital Video Recording System; Procedure-OP-5507-A,
Retrieving DVR Harddrives

Approved by: 
Director of Operations

Written by: Jim Merrill

AUDITING MONTHLY DMERS

Definitions:

"DMER" - digital master evidence record form.

Action By:

Action:

Operations
Assistant

1. **Sends** copies of the previous month's "DMERs" to the Human Resources Director.

Human
Resources
Director

2. **Reviews** relevant material for compliance with POLICY-OP-5507.

3. **Finds** material compliant.

4. **Notes** comments on FORM-OP-5507 and **notifies** Director of Operations and Fixed Route Manager. **Skips** to step 8.

- 4a. If issues or concerns with the DMERs, **documents** issues on FO-OP-5507, **notifies** the Director of Operations and **schedules** meeting the Fixed Route Manager.

5. **Meets** with Fixed Route Manager to discuss issues.

- 5a. If after discussion, **finds** materials to be compliant, **sends** written notification of compliance to Director of Operations and Fixed Route Manager. **Skips** to step 8.

- 5b. If materials determined NOT fully compliant with POLICY-OP-5507, **meets** with the General Manager and Director of Operations to discuss need for corrective action.

General
Manager

6. **Meets** with Fixed Route Manager to review violation and clarify appropriate practice.

Effective: June 7, 2007
Cancels: New

Page: 2 of 2

INTERCITY TRANSIT PROCEDURE-OP-5507-B

7. **Documents** discussion on FORM-OP-5507 and **forwards** form to Fixed Route Manager for filing.
 8. **Files** notification and any comments with the respective DMER.
- Fixed Route
Manager

Effective: June 7, 2007
Cancels: New

Page: 1 of 1

INTERCITY TRANSIT TASK-OP-5507-A

See Also: POLICY-EX-0005; TASK-EX-0005-B; FORM-EX-0005

Approved by: 
Director of Operations

Written by: Jim Merrill

RETAINING DVR SYSTEM RECORDED MATERIAL

Definitions:

"DVR system recorded material" – digital video and audio recorded material saved on the hard drive of a Digital Video Recording System.

"Digital Video Disc (DVD)" -High-density compact disk for storing large amounts of data.

After viewing the "DVR system recorded material," the **Fixed Route Manager:**

1. **Decides** to retain recorded material.
2. **Saves** the relevant segments of the recorded material to a secure server.
3. **Copies** the material in its original format to a "DVD."
4. **Places** the DVD, incident reports, dispatch logs, and any other related documentation in a single file and **labels** the file by date and route number.
5. **Stores** the file in a designated secure cabinet.
6. **Discloses** the material to the public upon request in compliance with the Public Records Act of the State of Washington, Chap. 42.56, and Intercity Transit POLICY-EX-0005.

Effective: June 7, 2007
Cancels: New

Page: 1 of 2

INTERCITY TRANSIT TASK-OP-5507-B

See Also: TASK-OP-5507-A; POLICY-OP-5507; FORM-EOP5507

Approved by: 
Director of Operations

Written by: Jim Merrill

REVIEWING DVR SYSTEM RECORDED MATERIAL

Definitions:

"DVR System Recorded Material" – video and audio recorded material saved on the hard drive of a Digital Video Recording (DVR) System.

"DMER" – DVR System Master Evidence Record Form.

To proceed with the investigation of a serious incident involving video and audio recorded material, the **Fixed Route Manager**:

1. **Receives** the DVR hard drive and DMER (FORM-OP-5507) from the Operations Supervisor.
2. **Views** the recorded material that corresponds to the incident.
3. **Maintains** confidentiality while reviewing materials.
4. **Determines** how to respond to the incident and **decides** the potential importance of the recorded material.
 - 4a. **Asks** Operations Director and/or legal counsel for assistance, if needed.
5. **Retains** copies of the recorded material when justified.
 - 5a. With advice of legal counsel, **retains** the hard drive itself as legal evidence if the seriousness of the triggering incident merits retention.
 - 5b. **Saves** the recorded material per TASK-OP-5507-A.
6. **Documents** decisions and actions on FORM-OP-5507 and **ensures** continued confidentiality of recorded material.
7. **Delivers** hard drive to Operations Supervisor for return to its assigned vehicle, PROCEDURE-OP-5507.

Effective: June 7, 2007
Cancels: New

Page: 2 of 2

INTERCITY TRANSIT TASK-OP-5507-B

See Also: TASK-OP-5507-A; POLICY-OP-5507; FORM-EOP5507

Approved by: _____
Director of Operations

Written by: Jim Merrill

- 7a. If hard drive is retained, informs Operations Supervisor to leave replacement hard drive in vehicle and documents on FORM-OP-5507.

Page: 1 of 2

See Also: N/A

Written by: Jim Merrill

y y y y m m d d h h m m r r r r r r r r r r c c c c

13. Event file initially reviewed by		NAME	DATE	SIGNATURE
14. Event file initially reviewed by <input type="checkbox"/> Digitally duplicated original file on CD-R/DVD-R disk <input type="checkbox"/> Leave on server				
File digitally duplicated on CD-R/DVD-R disk by		NAME	DATE	SIGNATURE
16. Additional CD-R/DVD-R disk(s) created by		NAME	DATE	SIGNATURE
17. Number of additional CD-R/DVD-R disks created				
18. Additional CD-R/DVD-R disks distributed to		NAME	DATE	SIGNATURE
NOTICE Neither the information on this form, nor the video and audio files on the accompanying CD-R/DVD-R disk(s) shall be released to an other person or persons without the expressed written permission of Intercity Transit or their designee.		NAME	DATE	SIGNATURE
		NAME	DATE	SIGNATURE
		NAME	DATE	SIGNATURE
		NAME	DATE	SIGNATURE
19. Digitally duplicated CD-R/DVD-R disk submitted as criminal evidence by		NAME	DATE	SIGNATURE
20. Evidence submitted to		NAME	DATE	SIGNATURE
21. Digitally duplicated CD-R/DVD-R disk submitted as tort evidence by		NAME	DATE	SIGNATURE
Evidence submitted to		NAME	DATE	SIGNATURE

13. Evidence submitted to

Memorandum of Agreement

Intercity Transit and ATU Local 1384

Pursuant to a demand to bargain submitted by the Union April 11, 2007, the parties entered into an "impact negotiations" on the affects of implementing a comprehensive on-board digital video recording system throughout the revenue fleet on May 14 and June 25, 2007.

The parties have agreed no recording shall be used by any manager against any ATU member for the purpose of finding misconduct or issuing discipline, referred to by the parties as "targeted surveillance" or "fishing," except where there is an initiating event such as a complaint, accident, incident or infraction and as referenced in Article IX, Section B of the labor *Agreement*.

To implement this agreement, the policy and procedures adopted by the Intercity Transit Authority on June 6, 2006 resolve the Union's concerns regarding "targeted surveillance", "fishing" and records maintenance. For example, the adopted policy and procedures permits viewing of recorded material to that which is associated with an "incident." As a result, "fishing" is not within the adopted policy and procedures.

These June 2007 policies and procedures included the following:

- POLICY-OP-5507
- PROCEDURE-OP-5507-A
- PROCEDURE-OP-5505-B
- TASK-OP-5507-A
- TASK-OP-5507-B
- FORM-OP-5507

The parties further agree that any audio record of a "protected" Union conversation shall not be used by any manager in a manner that would be contrary to the interest of a member of the bargaining unit.¹ The Union agrees to caution its stewards, officers, agents and members to exercise due diligence in protecting the Local's interests and the interests of its members.

In the event Intercity Transit plans to amend the above referenced policy and procedures, it shall notify the Union so the Union may submit a timely demand to bargain the impact of any such amendments. This provision includes any additional audio input device outside of the "fare box area" or a video input device that is focused on the "operator's compartment."



For Intercity Transit



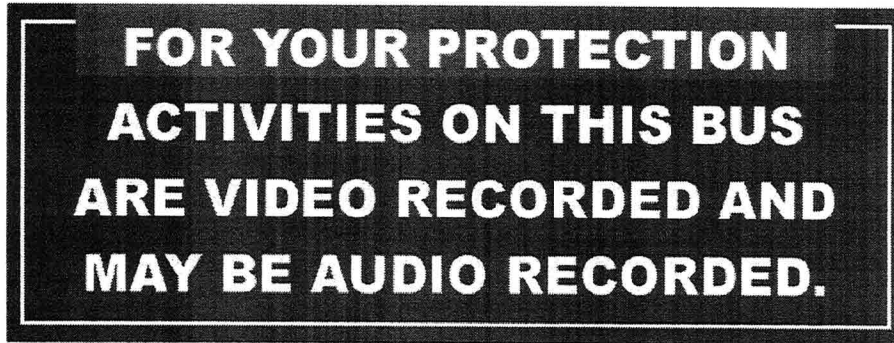
For ATU Local 1384

Date: 8/27/07

Date: 8/27/07

¹ The term, "protected" means that the conversation is member to member or member to officer or visa versa regarding issues of representation or lawful union business.

Signage on coaches and paratransit vehicles:



Signage at facilities:



**Lehigh and Northampton Transportation Authority (LANTA),
Allentown, Pennsylvania**

Video Surveillance/Camera Maintenance Policy

45

VIDEO SURVEILLANCE/CAMERA MAINTENANCE POLICY

Effective January 01, 2017

The Lehigh and Northampton Transportation Authority places the highest priority on employee, passenger, and public safety. Placing video cameras on Authority vehicles and properties is one way to ensure employee and passenger safety, proper asset management and general security for the authority and the public as to its vehicles and their operation, as well as to authority facilities.

I. Posting Guidelines:

The Authority shall post notices on each vehicle and on its properties where cameras are located. There shall also be notification of the use of audio controls if that technology is utilized.

II. Ownership of Videos:

A. The ownership of video tapes from Authority vehicles or property rests exclusively with the Authority.

B. In the case of accident investigations and/or criminal investigations the Authority may provide videos to its solicitor, insurance adjuster, Law Enforcement, and other persons who may require the use of such video to defend the authority.

C. Nothing in this policy should be construed to provide additional rights as to the review and/or duplication video tapes under the Pennsylvania Right to Know Act. Any and all exceptions as to the review and/or duplication of tapes under the Right to Know Act remain applicable to all videos.

III. Viewing Policy:

A. The Authority may view cameras for any reason including performance reviews of employees, accident investigation, investigation of passenger and/or employee complaints, camera maintenance and/or testing, criminal investigation purposes or other reason determined by the Authority as to the necessity to review videos.

B. The Authority shall designate the Executive Director, Deputy Executive Director, Director of Operations, Senior Operations Supervisor, Human Resources Manager, and any other personnel authorized by the Executive Director or Director of Operations as the person's privy to the review of videos.

C. The Authority may use vehicle and/or property cameras as a method of cooperating with law enforcement personnel to investigate accidents, crimes or other activities upon request of such a law enforcement officer. The decision to allow law enforcement officers to review videos shall rest with the Authority's Executive Director.

IV. Video Retention:

A. In the event of accident investigation retention, such videos shall be retained for a period of three years after the event or until such time as litigation has come to an unappealable resolution.

B. In the event that a video is retained for any other purpose, the Authority shall refer to its record retention policy.

C. Videos shall be retained in a manner that protects any digital and/or taped video format based upon available technology at the authority.

V. Maintenance:

A. The Authority shall check the operation of its video cameras at each 6,000 mile maintenance review.

B. Operators or maintenance personnel shall report malfunctioning cameras at a minimum, at the conclusion of the shift on which the discovery is made concerning the functionality of such camera.

C. The Authority shall not make it a practice of checking cameras on daily pre-trip and/or post-trip inspections.

D. The Authority shall use its best efforts to ensure that its cameras are operational on a daily basis. However, due to the mechanical nature of cameras the Authority cannot guarantee the operation of one or more vehicle cameras at any given time.

Massachusetts Bay Transportation Authority, Boston, Massachusetts

Policy on MBTA Video Access, Distribution, & Retention

46



SECURITY & EMERGENCY MANAGEMENT DEPARTMENT POLICY ON MBTA VIDEO ACCESS, DISTRIBUTION, & RETENTION

Updated March 20, 2014

The Massachusetts Bay Transportation Authority operates video surveillance cameras across its many stations, facilities, parking lots, and vehicles. These cameras are used to enhance system safety and security and are operated and managed in strict accordance with the access, distribution, and retention practices detailed in this policy. This policy was developed with the objective of balancing operational needs, privacy concerns, and storage costs.

1.0 VIDEO ACCESS AND PRIVILEGES

The MassDOT Security & Emergency Management Department is responsible for managing all users' access to the MBTA Video Management System ("VidSys"), which offers both live and recorded video feeds from surveillance cameras.

1.1 SYSTEM ACCESS

Users must request access to the MBTA Video Management System from the MassDOT Security & Emergency Management Department. The Department reviews all requests and issues dedicated user accounts to those with a verified need for access to the system. Authorized users are then issued dedicated video workstations for accessing the MBTA's specialized video management software.

Refer to Attachment "MBTA VidSys Access Request Form"

1.2 SYSTEM PRIVILEGES

Based on user needs, appropriate department officials may be granted access to all cameras (super and executive users), or cameras only in areas relevant to their geographic or functional responsibilities (regular users). For example, a Hub Center will not have access to ITD data centers and the IT Department will not have access to Transit Police Department areas.

To all authorized users, the Department issues dedicated video workstations and accounts for accessing the MBTA's specialized video management software. Users can access both live and recorded footage for the cameras they have access to.

2.0 VIDEO DISTRIBUTION

While multiple departments across the MBTA have access to view live and recorded video within the MBTA's video management software, only the Security & EM Department and the MBTA Transit Police Department have the ability to export video from this system for external distribution. This is by design to control and limit video recording distribution.

2.1 VIDEO RELATED TO CRIMINAL ACTIVITY

The MBTA Transit Police is responsible for all video requests and distribution related to criminal activity. This includes interaction with the court system and external public safety agencies.

2.2 VIDEO NOT RELATED TO CRIMINAL ACTIVITY

The MassDOT Security & Emergency Management Department handles all video requests and distribution duties for video that is not related to criminal activity. In this capacity, other MBTA departments may request specific video clips from the Security & Emergency Management Department by submitting an appropriate written request. This request must take the form of a completed "MassDOT Security & EM Department Video Request Form" that provides justification for the release and is signed by the head of the requesting department.

All requests are vetted by the Department based on operational needs. If approved, a video clip is generated and provided electronically via the MBTA network or on a CD-ROM. Any video obtained may be privileged and confidential, and is for the official use of the MBTA only. In addition, all requests are logged and archived for later reference.

In addition to processing requests from other departments, the MassDOT Security & Emergency Management Department also proactively reviews Operations Control Center Dispatcher reports to identify and locate video relevant to incidents that may impact employee, legal, and workers compensation issues.

Refer to Attachment "MassDOT Security & EM Department Video Request Form"

3.0 VIDEO RETENTION

It is the general intention of the MBTA to retain 30 days of recorded video, with the following important caveats:

- Existing bus vehicle cameras are currently equipped to store video locally (on-board hard drives) and therefore may only support a maximum of 10 days of video. Because video recording is triggered by motion, a bus that has seen heavy use in a given period may only allow for as little as 3-4 days of video. These older vehicle camera systems are gradually being enhanced with wireless storage capability that will enable 30 day retention of video related to an on-board incident.
- In some cases, industry or regulatory requirements obligate the MBTA to retain more than 30 days of video. For example, PCI requirements necessitate up to 90 days of video retention at data centers and revenue facilities.
- The MassDOT Security & Emergency Management Department also has determined that certain cameras related to critical infrastructure or highly sensitive areas may be recorded for longer periods of time.

The MBTA has dual recording capability. As such video is stored in secure, climate controlled data centers at our primary site and secondary sites. Additional video retention redundancy is made possible via local video recorders situated at the various transit stations and key facilities.

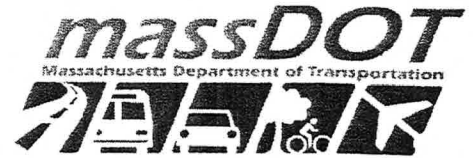
4.0 POLICY REVISIONS

This policy will be reviewed annual and updates and distributions will occur as needed. If individuals have comments or questions related to this policy can contact the Security and Emergency Management Department via email at securitydepartment@mbta.com


Randy Clarke

Senior Director of Security &
Emergency Management

03/20/14
Date



SECURITY & EMERGENCY MANAGEMENT DEPARTMENT VIDEO ACCESS REQUEST FORM

Updated January 2, 2013

MassDOT personnel seeking to obtain records from MassDOT video systems to fulfill a specific job-related function must use this form. E-mail this fully completed form to securitydepartment@mbta.com.

MassDOT allows the release of records from active video systems to MassDOT personnel on a "need to know" basis in connection with operational and/or legal obligations/responsibilities. By having MassDOT personnel submit this form, MassDOT is making a reasonable effort to limit the scope of the disclosure, restricting such disclosures only to appropriate personnel and disclosing only such records as are reasonably required to fulfill the purpose of the disclosure in connection with a specified MassDOT-related function. The records obtained as a result of submitting this form may be privileged, confidential and for the official use of MassDOT only.

REQUESTER INFO

NAME: _____ EMPLOYEE #: _____
TITLE OR POSITION: _____
MASSDOT DIVISION: _____ DEPARTMENT: _____
PHONE #: _____ E-MAIL: _____

VIDEO REQUESTED

PURPOSE OF VIDEO REQUEST: _____
DESCRIPTION OF INCIDENT: _____
DATE OF INCIDENT: _____ LOCATION: _____
TIME (START) _____ TIME (END): _____
CAMERA #/NAME: _____

CERTIFICATION

The undersigned acknowledge and agree that the records provided pursuant to this request are protected and restricted to MassDOT personnel only and unauthorized disclosure is strictly prohibited.

REQUESTER:	_____ SIGNATURE	_____ PRINT NAME	_____ EMPLOYEE #	_____ DATE
DEPARTMENT HEAD:	_____ SIGNATURE	_____ PRINT NAME	_____ EMPLOYEE #	_____ DATE

SECURITY & EMERGENCY MANAGEMENT DEPARTMENT USE ONLY

ID: _____

[] VIDEO NOT RELEASED DATE: _____ REASON: _____
[] VIDEO RELEASED DATE: _____ RELEASED BY: _____

Metropolitan Atlanta Rapid Transit Authority (MARTA), Atlanta, Georgia

Department of Police & Emergency Management, Authority-Wide
CCTV Policy

48



METROPOLITAN ATLANTA RAPID TRANSIT AUTHORITY

DEPARTMENT OF POLICE & EMERGENCY MANAGEMENT

AUTHORITY-WIDE CCTV POLICY

**PREPARED BY: WANDA Y. DUNHAM, AGM
CHIEF OF POLICE & EMERGENCY MANAGEMENT**

March 2016



marta	POLICY	ISSUE DATE 03-31-2016 Revision No: 00	REFERENCE NO. PS-PO-2020	Page 2 of 14
TYPE : Authority-Wide CCTV Policy				

TABLE OF CONTENTS

I.	General	3
A.	Scope	3
B.	Purpose	3
C.	Review	3
D.	Definitions	4
E.	Responsibilities/Applicability	5
II.	Policy/Resolution	5
A.	Police Authority and Responsibility for Managing the System and Granting Access	5
B.	Roles of Other Parties in Managing the CCTV System Generally	7
C.	User Groups	7
D.	Reporting of Problems, Misuse and Policy Violations	8
E.	Training	8
F.	Download of Live and Stored Video	9
G.	Release of Video Data	10
H.	Video Requests Originating Other than for Usual User Group Purposes	10
I.	CCTV-Specific Policies	11
1.	Camera Naming and Description Conventions	11
2.	Use of Fixed and PTZ Cameras	11
J.	VSCS-Specific Policies	11
1.	VSCS Reporting Requirements for Employees and Contractors	11
2.	VSCS Hard Drive Protection and Vehicle Operation	12
3.	DVR System Access Key Control	12
K.	System Modifications and Maintenance	13
III.	Compliance	13
IV.	Supporting Documents	14

marta	POLICY	ISSUE DATE 03-31-2016 Revision No: 00	REFERENCE NO. PS-PO-2020	Page 3 of 14
TYPE : Authority-Wide CCTV Policy				
ISSUING DEPARTMENT: Police And Emergency Management				
PREPARED BY: Police And Emergency Management				
APPROVED BY: <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 45%;"> <p>Wanda Y. Dunham AGM, Chief of Police & Emergency Management</p> <p>Elizabeth O'Neill, Esq. Assistant General Manager, Legal Services</p> <p>Edward Johnson Chief Administrative Officer</p> <p>Keith T. Parker, AICP General Manager and Chief Executive Officer</p> </div> <div style="width: 45%; text-align: right;"> <p><i>Wanda Y. Dunham</i> 5/11/16 Signature Date</p> <p><i>Elizabeth O'Neill</i> 2-9-16 Signature Date</p> <p><i>Edward Johnson</i> 12-2-16 Signature Date</p> <p>DocuSigned by: <i>Keith T. Parker</i> 5/11/2016 Signature Date E91F232A469F465</p> </div> </div>				
SUPERSEDES: This is the original version of the Authority-wide Policy. It supercedes the 2010 Police and Emergency Management CCTV Policy				

I. General

A. Scope


This document covers Authority-wide policy for all MARTA personnel related to MARTA's closed-circuit television (CCTV) and Vehicle Security Camera System (VSCS) system. For purposes of this Policy, the term "CCTV system" includes and applies to both CCTV and VSCS, except as specifically distinguished because of differences between the two.

B. Purpose

The CCTV Policy, together with the video technology it supports, is intended to promote a safer and more secure environment and to reduce the cost and time of investigations related to criminal activity, accidents, injuries, safety violations and customer complaints.

C. Review


The contents of this document will be reviewed by 5/1/2016 and by 5/1 of each year thereafter. The System Administrator, Technical Administrator, and any Policy Group then in existence will review this document with recommendations for revisions forwarded to the AGM/Chief of Police and Emergency Management and the AGM of Legal Services by 5/1.

 POLICY	ISSUE DATE 03-31-2016 Revision No: 00	REFERENCE NO. PS-PO-2020	Page 4 of 14
TYPE : Authority-Wide CCTV Policy			

D. Definitions

The following terms, abbreviations and acronyms are associated with this Policy.

TERM	DEFINITION
Archive	The automatic storing of CCTV-specific video and related data, which is usually retained for a maximum of 30 days.
CCTV (Closed Circuit Television)	MARTA's cameras, computers and network which acquire, transmit, display, and store video data using closed-circuit television technology
CCTV system	Term which, for convenience in this CCTV Policy, includes both VSCS and CCTV equipment, network, video and data.
CCTV Policy Group	One of what may be multiple groups appointed by the Chief of Police and Emergency Management.
Download	The process of copying video footage from CCTV system storage to other electronic media.
DVR (Digital Video Recorder)	VSCS-specific computer which houses and reads and writes to Hard Drives and communicates with vehicle cameras and the VSCS servers. Each bus, van and train car with cameras has a DVR. Several departments, including MARTA Police, Legal Services, Safety and the garages also have DVRs for reviewing and downloading data from Hard Drives.
Fixed Camera	A camera that has a single view/focus that may not be modified on a "live" basis.
Group Manager	Designated person(s) for each User Group responsible for coordinating between the User Group members, the System Administrator and System Technical Administrator.
Hard Drive (note capitalization)	Combination of a computer hard drive and a metal enclosure with connectors which mate with connectors within DVRs to allow easy removal and replacement. Each VSCS-equipped bus, van or train car is paired with a specific Hard Drive.
IT	MARTA Information Technology Department.
Live View	A VSCS function permitting the authorized user to view the camera feeds from revenue vehicles remotely, in a "live" environment, through a cellular connection
Maintenance	The work of configuring the CCTV system, repairing cameras and/or addressing software and connectivity issues.
Metadata	Data that comes along with, or is used to manage, control or log, the primary video data. The CCTV system includes two primary types of metadata: (1) metadata stored with video, such as time, date, camera, location, speed and accelerometer; and (2) system metadata, such as data which is used to locate, log the status of, and manage the video files.
PTZ (Pan/Tilt/Zoom)	Feature available on select CCTV camera models that gives a remote user the ability to remotely reposition and refocus the camera view.

 POLICY	ISSUE DATE 03-31-2016 Revision No: 00	REFERENCE NO. PS-PO-2020	Page 5 of 14
TYPE : Authority-Wide CCTV Policy			

TERM	DEFINITION
Recording	Saving real-time video footage on an electronic storage device, such as a hard drive.
Staff member	Employee or contractor with various levels of CCTV system access and/or responsibility.
Supervisor	A person granted access to view live and archived video, record live video, download archived video and control a PTZ camera.
System Administrator	A member of the MARTA Police and Emergency Management Department who administers the CCTV system and manages staff member access rights.
Technical Administrator	A member of the Department of Technology (IT) responsible for the technical administration of the CCTV system.
Upload	The sending of VSCS audio, video, and/or other metadata by the on-board vehicle DVR to the server(s).
User	A person authorized to only access the "Live View" feature of the CCTV-specific cameras.
User Group	A group of staff members who have been granted some level of CCTV access.
VSCS (Vehicle Security Camera System)	System of cameras and related network, software and servers to capture and store video from certain MARTA revenue vehicles.

E. Responsibilities/Applicability


The individuals responsible for performing this guideline are

- The System Administrator
- The Technical Administrator
- The AGM/Chief of Police and Emergency Management and
- Every person who works with any component of, or data resulting from the operation of, the CCTV system.

II. Policy/Resolution

A. Police Authority and Responsibility for Managing the System and Granting Access

The CCTV system, Authority-wide, is managed by the MARTA Police and Emergency Management Department. The MARTA Chief of Police and Emergency Management or his/ her designee have the highest level access rights and have full access and control rights to all cameras, stored video, and PTZ controls, including the ability to lock and control any camera at any time. The MARTA Chief of Police and Emergency Management is responsible for (1) granting access to MARTA employees and contractors as appropriate for MARTA's business activities and (2) the administration of this system, as described in this Policy, including delegating to the System Administrator and Technical Administrator and other designees as appropriate.

	POLICY	ISSUE DATE 03-31-2016 Revision No: 00	REFERENCE NO. PS-PO-2020	Page 6 of 14
TYPE : Authority-Wide CCTV Policy				

The MARTA Chief of Police and Emergency Management routinely grants ongoing CCTV access to members of User Groups below if doing so supports MARTA's business functions and does not compromise security. Access may be denied or removed if security is compromised or misuse of the system occurs.

The **System Administrator** is responsible for the overall administration of the CCTV system, for reviewing requests for access, for submitting such requests to the Chief of Police and Emergency Management, for retaining and organizing signed access requests, for maintaining the master list of all persons with access rights and level of access rights, and for providing copies of such documents and master list to other persons when requested, such as Training, Safety, and Group Managers. When access has been approved for any person, the **System Administrator** is responsible for providing written documentation to the Technical Administrator and notice to the person granted access and to whoever will provide training that (a) access has been granted and (b) training is necessary before the trainer can give the person a log-on password and actual access.

The **System Administrator** and the **Chief of Police and Emergency Management Services** shall make arrangements for a member of Police and Emergency Management Services to be delegated authority to act on behalf of the System administrator in his/her absence.


Upon the decision to remove someone from access, the **System Administrator** will notify the staff member that they will be removed from the master list and request the Technical Administrator to configure the system not to accept the staff member's log-in.

The **MARTA Police and Emergency Management Department** is responsible for reviewing weekly CCTV update reports and coordinating with the Technical Administrator and other stakeholders supporting and using the CCTV system.

In managing the CCTV system, MARTA follows the MARTA SEPP (Security and Emergency Preparedness Plan). The SEPP reflects the Authority's commitment and inter-departmental approach to ensuring the safety and security of the MARTA transit community and employees.

The **Chief of Police and Emergency Management Services** may, either for specific purposes for a limited time, or on an on-going basis, appoint **CCTV Policy Groups**. Purposes for such Groups may include monitoring the CCTV system and its use, evaluating policy issues, assisting in development of the CCTV system, providing technical expertise, providing or obtaining input from different user and affected groups, assisting in addressing specific problems or concerns, and/or making recommendations. Any such Group serves at the discretion of the Chief of Police and Emergency Management, who serves an ex-officio member, and who has the discretion to serve as chairman and/or dissolve any Group at any time.

Documentation and information concerning the CCTV system is considered security sensitive information (SSI). SSI includes but is not limited to specifications, use, design, layout, quantity of cameras, field of view, MARTA internal reports concerning the CCTV system, maintenance records, and camera locations. Requests for such information from someone not in a User Group must be in writing using a CCTV Access Request Form with a detailed justification and must receive final approval from the Chief of Police prior to release of any data. Persons in User Groups who have such SSI information or documentation have no authority to release it, except as necessary to legal and administrative proceedings or with specific written authorization from the System Administrator or Chief of Police and Emergency Management. Note that this paragraph does not cover video or metadata related to specific video, which is discussed elsewhere in this document.

 POLICY	ISSUE DATE 03-31-2016 Revision No: 00	REFERENCE NO. PS-PO-2020	Page 7 of 14
TYPE : Authority-Wide CCTV Policy			

B. Roles of Other Parties in Managing the CCTV System Generally

Through direction from the Technical Administrator, MARTA IT is responsible for updating and managing the software, network and hardware associated with the CCTV system [See Appendix A].

Upon receiving signed access authorization from the **System Administrator**, the **Technical Administrator** sets up access consistent with the authorization and provides a log-on password to the person who will train the staff member. Upon the decision to remove someone from CCTV access, the **Technical Administrator** removes the staff member from the master list and configures the system to not accept the staff member's log-in.

The **MARTA Radio Maintenance Department** is responsible for physically checking all cameras on the CCTV system, both physically and using CCTV, and making repairs to broken or malfunctioning cameras and their connections and wiring from the cameras to the local router and/or computer at the location [See Appendix B].


MARTA Police, IT and Radio Maintenance must coordinate to ensure that the CCTV system is fully functional at all times, consistent with the MARTA SEPP. Camera malfunctions will be addressed as provided in Appendix A and Appendix B. See also System Modifications and Maintenance below.

At the time of preparation of this version of the CCTV Policy, **MARTA IT** supplies, supports and maintains the physical computer servers and network for the VSCS, but, because the VSCS contract is not complete, most of the components of the VSCS are still owned by the VSCS vendor, Apollo Video Technology ("Apollo"). Until contract completion and handover, Apollo still has primary responsibility for all its components of the VSCS, with various MARTA departments assisting with maintenance and testing as agreed between MARTA and Apollo.

C. User Groups

Specific User Groups have authority, as granted by the Chief of Police and Emergency Management, to access and/or store video and related data as part of MARTA's business activities. Staff members in User Groups may be limited to authority to use and manage specific cameras or groups of cameras for a specific purpose. **User Groups** are authorized to add this plan or parts thereof to their existing operating procedures and may develop additional internal procedures which do not conflict with this plan. Presently recognized User Groups are:

- Bus Operations
- Emergency Management (EOC) | Terrorism Prevention
- General Manager's Office
- Information Technology
- Legal Services
- Police Services
- Radio Maintenance
- Rail Operations
- Risk Management
- Station Services

	POLICY	ISSUE DATE 03-31-2016 Revision No: 00	REFERENCE NO. PS-PO-2020	Page 8 of 14
TYPE : Authority-Wide CCTV Policy				

- System Safety
- Treasury Services

Staff members must access the CCTV system for official MARTA business use only. No camera, video or CCTV equipment should at any time, under any circumstance, be used for recreational, personal or non-MARTA-business pecuniary purposes.

If an incident requires Police video surveillance, investigation and/or involvement, all other User Groups have a lesser priority than Police and Emergency Management. User Groups may not hinder, obstruct or deny the viewing of any live or archived footage requested by or currently being viewed by the MARTA Police and Emergency Management Department.

Each User Group must have at least one **Group Manager** responsible for coordinating between the User Group members, the System Administrator and System Technical Administrator.

Group Managers are also responsible for reporting any misuse of the CCTV system to the System Administrator, and reporting any technical failures to the Technical Administrator through an IT service request.

D. Reporting of Problems, Misuse and Policy Violations

MARTA employees and contractors who review video and related data are responsible for reporting, to MARTA Police and Emergency Management or to MARTA supervisors as appropriate, observations of criminal or suspicious behavior and activities which violate MARTA policy.

All MARTA employees and contractors should immediately report to a MARTA supervisor (a) any accident or incident which may give cause for downloading/storing video, or (b) failure or malfunction of any CCTV system component. Employees, supervisors and management with access to do so should report:


- any accident or incident which may give cause for downloading/storing video to bus, rail or Mobility communications control, to Legal Services or Risk Management as appropriate and
- any failure or malfunction of any CCTV system component to the MARTA IT help desk.

MARTA employees who discover that a CCTV system component has been rendered non-operational through intentional unauthorized actions (including but not limited to cameras being taped over or turned off) shall immediately document their observations and report them by calling the MARTA Police Department.

MARTA employees with knowledge of any accident or incident for which video should be preserved, or knowledge of disabling or attempted disabling of CCTV system components, shall support the investigation and, if possible, include with their report photographs of the damage or evidence of the attempt to disable equipment. These can be sent directly to MARTA Police through the See & Say mobile application or by another method supported by the MARTA Police Department.

In the event an entire train station, garage or similar large system failure occurs, any employee with knowledge of the failure should immediately notify the MARTA Police & Emergency Management Department.

E. Training

 POLICY	ISSUE DATE 03-31-2016 Revision No: 00	REFERENCE NO. PS-PO-2020	Page 9 of 14
TYPE : Authority-Wide CCTV Policy			

All personnel operating, maintaining and administering the CCTV system must be trained in the functions that they will be performing. Training consists of the courses listed below.

Upon receiving approval from the System Administrator and a password from the System Technical Administrator, **the trainer** will schedule the appropriate training for the staff member. Upon completion of the training, **the trainer** will provide the staff member with a log-on password and notify the System Administrator, who will add the staff member to the master list of personnel who have access, as well as documenting the staff member's level of access.

The training curriculum should include a review of the most updated version of this Policy. Training should also include providing contact information for the current System Administrator and Technical Administrator and how to report camera and system failures.

- a. User Training is provided for staff members who only have access to view the CCTV system live. This training will cover the use of the CCTV-specific application software for live viewing.
- b. Supervisor Training is provided for staff members granted access to view live or stored video, to operate PTZ cameras and return them to default settings, to download archive video or record live video to permanent storage. This training covers the use of the CCTV application software, the cameras, camera controls, accessing stored video and permanent storage features.
- c. Maintenance Training is provided for staff members who maintain the camera hardware. This training will cover the use of the CCTV application software, the cameras, camera controls, how to maintain and repair the camera hardware, and how to make physical connections between cameras, computers and the network.
- d. Administration Training is provided for users who need to maintain and configure the network system, servers and video/data storage. This training will cover CCTV system application software, cameras, camera controls, and also how to maintain, repair and configure the network system and workstations connected to the CCTV system. Administration training may be limited, for particular staff members, to those components the staff member will be maintaining and/or configuring.


F. Download of Live and Stored Video

Note that, due to the technical complexity and high storage requirements of digital video, MARTA cannot ensure that video is available for any set period of time following an incident.

CCTV-specific video is usually stored for a maximum of 30 days ("archived"), after which it is automatically deleted through an overwrite process.

VSCS video and data is stored in hard drives on each vehicle. The VSCS is designed to overwrite older video as the hard disk drive fills to capacity. The overwriting process is completed on a "first-in first-out" continuous basis. On-board storage retention varies based on the number of cameras, resolution settings, hard drive capacity, and the number of hours per day the vehicle is turned on. VSCS retention varies depending on these variables, but generally is between 12 to 15 days.

Access to download live or stored video ("download access") is only given on an ongoing basis to those staff members who have been given Supervisor level access as approved by the Chief

 POLICY	ISSUE DATE 03-31-2016 Revision No: 00	REFERENCE NO. PS-PO-2020	Page 10 of 14
TYPE : Authority-Wide CCTV Policy			

of Police Services and Emergency Management. The primary criterion for download access is job need, but other considerations include safety, security, crime prevention, legal and administrative proceedings, Open Records Act compliance, customer service and operations. Download access may be withheld if security may be compromised or misuse of the system has occurred.

Staff members in the following User Groups are routinely granted ongoing Supervisor-level access to download video and data from the CCTV system unless there is a reason for an exception, such as misuse of the CCTV system by an individual: Police Services, Emergency Response Coordination/Terrorism Prevention, the General Manager's office, Legal Services, Safety, and Risk Management. Download access may also be granted to Group Managers and to other persons selected by Group Managers or by the System Administrator under appropriate circumstances, as described in the preceding paragraph.

Video and related data which may be needed as part of a police investigation or for evidence in criminal proceedings, or if it includes PTZ camera views, should follow appropriate chain of custody procedures, including but not limited to: downloading to a removable storage media, processing as an item of evidence, logging in an evidence log and storing in a secure location with access by authorized personnel only. The log shall at a minimum include the person who requested and who performed the video download, the reason for the video download and a contact person with knowledge as to when the video can be destroyed.

G. Release of Video Data

MARTA employees and contractors shall not disseminate video, related data or information learned from viewing CCTV video unless such release is authorized by the Chief of Police and Emergency Management Services, the AGM of Legal Services or the General Manager, or video or data is required to be released or provided to other parties as part of legal or administrative proceedings or by the Open Records Act.

Employees may obtain a form to request permission to release video from the System Administrator.

H. Video Requests Originating Other than for Usual User Group Purposes


MARTA employees and contractors who seek video, but do not have Supervisor/download access, should submit a written request to Legal Services as soon as the need is known. The request shall include a reason, consistent with this Policy, for the request.

Download requests made by the general public shall be processed by Legal Services in accordance with the Open Records Act.

Download requests made by non-MARTA police departments should be directed to the MARTA Chief of Police and Emergency Management or the System Administrator.

Whenever practical to do so, requestors should be informed, at the time of the request, that, due to the many technical difficulties of taking, storing and downloading video, video is not always available, even if cameras were present.

Download requests must be prioritized so that, if possible, they can be processed before video is automatically deleted. Video clips provided to requestors on portable media should be accompanied by a copy of the written request.

 POLICY	ISSUE DATE 03-31-2016 Revision No: 00	REFERENCE NO. PS-PO-2020	Page 11 of 14
TYPE : Authority-Wide CCTV Policy			

If requested video cannot be obtained, or if the request for video is denied, the physical request form must be completed showing (1) the efforts made to obtain the video, by whom and why the video cannot be obtained, or (2) the reason the request is denied, and by whom. A copy of the request form should be sent promptly to the requestor within a reasonable time after (a) video is retrieved (b) MARTA finds that the requested video cannot be retrieved or (c) the request is denied.

I. CCTV-Specific Policies

1. Camera Naming and Description Conventions

Each CCTV camera has a five-character number, IP Address and description assigned by IT.

Each camera description field has a description of its location, area of focus and primary view. For example, if the camera's primary view includes a particular bus route loading/unloading area, then the bus route number(s) is included in this text. **MARTA IT** is responsible for keeping the description field accurate, such as changing the description text when a bus route in such text is relocated.

2. Use of Fixed and PTZ Cameras

Fixed cameras show a single view. An example is a camera positioned to capture patron movement on an escalator.

PTZ cameras are used to monitor an area. Each PTZ camera has a default position/focus. A PTZ camera might, for example, be set so it could be repositioned to monitor patron movement through any of the doors of a train. Such a camera's default view might be a view likely to capture several doors at the same time.

The archive system only records the view the PTZ cameras have at the time of recording. Any PTZ camera moved away from its default view by any staff member should be returned to default view by the staff member.

J. VSCS-Specific Policies


This portion of the CCTV Policy is intended to ensure, as much as is practically possible, that MARTA VSCS-equipped vehicles are not operated without a properly functioning DVR, cameras and the specific Hard Drive assigned to that specific vehicle.

1. VSCS Reporting Requirements for Employees and Contractors

When any employee or contractor, including any vehicle operator, discovers the VSCS is not operational through visual inspection (whether pre-trip, during operations, or post-trip), they should report the VSCS status to maintenance or to Bus, Rail or Mobility communications control as appropriate for further direction. With limited exceptions, the vehicle should be taken out of service if the VSCS is not operational. At the time of preparation of this version of the CCTV Policy, the VSCS equipment is generally not operational if the Event Switch is solid red or is not lit at all, if the public viewing monitor is not functioning, or if one of the four cameras views is black.

Any MARTA personnel who reports a VSCS malfunction or failure should provide the following information:

- a. Vehicle Number, Route

 POLICY	ISSUE DATE 03-31-2016 Revision No: 00	REFERENCE NO. PS-PO-2020	Page 12 of 14
TYPE : Authority-Wide CCTV Policy			

- b. Date and time malfunction was identified
- c. Nature of the malfunction if known (indicator light/monitor)

2. VSCS Hard Drive Protection and Vehicle Operation

Each vehicle is assigned a specific Hard Drive. MARTA cannot practically locate the video it needs unless the specific Hard Drive is in the correct vehicle and remains in that vehicle, except as provided below.

No vehicle shall enter revenue operations without its specific, assigned Hard Drive in service. Appropriate procedures must be put in place by the transportation and/or maintenance offices to ensure a vehicle is tagged or otherwise identified if the Hard Drive has been removed or is not recording video so that the vehicle does not go into service.

"Spare" hard drives should only be used in place of the original, assigned Hard Drive as a necessary, long-term replacement, such as when the original Hard Drive fails or Police and Emergency Management takes the Hard Drive for use in evidence. In that event, the "spare" Hard Drive becomes the assigned hard drive for long-term use. The replacement of any Hard Drive must be reported immediately to the Technical Administrator or System Administrator.

"Spare" Hard Drives should not be used on a temporary basis while a vehicle's assigned Hard Drive is taken out temporarily, such as for viewing or testing. Such a practice creates gaps in recording on the assigned Hard Drive, and MARTA has no practical way to track what video may be kept on a "Spare" temporary replacement.


To the extent it is practical to do so, VSCS-equipped vehicles should be operated even in non-revenue service, such as mechanical repair and cleaning, only if the assigned Hard Drive is in place and functioning properly.

3. DVR System Access Key Control

Control of the Hard Drives is critical to system function and security. Hard Drives on vehicles are locked within their DVR, which is in turn locked in a metal cabinet.

Only approved personnel in Police and Emergency Management, Department of Technology, Department of Safety and the Radio Maintenance shop shall have access to the VSCS file storage equipment on board a vehicle.

The stock supply of keys shall be maintained by a person with authorization granted by the Chief of Police and Emergency Management. The Chief of Police or a designated representative shall be responsible for approving the distribution of the keys upon receiving a written request. The written request shall include the requestor's name, title, supervisor's name, and the reason for the request. The requestor shall also identify the location where the key will reside. The MARTA Police Fleet Coordinator Officer shall maintain a "Key Inventory Log" identifying the approved distribution of keys including, at a minimum: Key Holder's name, title and phone number, supervisor's name, title and phone number, date request received, date key distributed, key number, and date key returned. Upon approval of the written request, the requestor shall pick up the key from MARTA Police. The key is to be used only for official use by the person to whom it is assigned and must be returned to MARTA Police after the assignee has vacated his or her role requiring its possession. Only MARTA employees from the Police, Safety, Legal, Risk Management, Radio Maintenance and necessary Bus, Mobility and Rail Departments, as approved by the Chief of Police and

 POLICY	ISSUE DATE 03-31-2016 Revision No: 00	REFERENCE NO. PS-PO-2020	Page 13 of 14
TYPE : Authority-Wide CCTV Policy			

Emergency Management, should be in possession of a key. The MARTA Police Department will periodically audit the key release log against the key inventory to track key distribution.

K. System Modifications and Maintenance

MARTA Radio Maintenance views and monitors the CCTV system Monday through Friday to identify CCTV problems or outages. Radio Maintenance is the first responder to trouble calls involving the CCTV system. Radio Maintenance generates daily reports and work orders which list all camera outages and work orders. The report is sent to the System Administrator and other interested parties on a distribution list on a weekly basis. [See Appendix B]

MARTA IT is responsible for server, network and software functionality. IT also monitors local archive servers and TCR master archive servers in order to maintain roughly 30 days of CCTV-specific archived video. [See Appendix A].

No changes shall be made to any existing CCTV system component without the prior approval of the System Administrator. Normal maintenance and repair may take place without prior approval, but a summary description of the actions taken must be submitted to the System Administrator and IT within 24 hours after normal maintenance and repair has occurred.

Any inoperable camera should be immediately reported to MARTA Radio Maintenance by contacting the IT help desk. If the problem cannot be solved by Radio Maintenance after being notified by IT, then Radio Maintenance should forward the ticket to MARTA IT for follow up related to the server and/or network.

Any person or department proposing to take cameras out of service must beforehand advise the System Administrator of a reason for the outage and projected time out of service, and obtain permission to do so.

III. Compliance

1. Employees (represented and non-represented) and contractors are prohibited from gaining unauthorized use or access to the CCTV system. Employees found in violation are subject to the following disciplinary action:

First Offense: Suspend three (3) days


Second Offense: Discharge

2. Authorized staff members are required to use the CCTV system in the manner for which they have been authorized. Unauthorized methods include but are not limited to the recording of images/videos with another device for the purposes of bypassing stated policies or procedures. Employees found in violation are subject to the following disciplinary action:

First Offense: Suspend three (3) days

Second Offense: Discharge

3. Employees and contractors are prohibited from unauthorized use and from unauthorized transferring or copying of CCTV system video, audio or metadata. Unauthorized use includes, but is not limited to, for example, unauthorized posting of video on the Internet and downloading video for personal, non-business reasons. Employees found in violation are subject to disciplinary action under MARTA's Personnel Policies regarding Conditions of Employment up to and including termination.

	POLICY	ISSUE DATE 03-31-2016 Revision No: 00	REFERENCE NO. PS-PO-2020	Page 14 of 14
TYPE : Authority-Wide CCTV Policy				

4. Employees are prohibited from unauthorized interfering with the function of any CCTV system component, including but not limited to disconnecting systems or power to systems, taping over camera lenses, and intentionally damaging CCTV system equipment. Employees found in violation are subject to disciplinary action under MARTA's Personnel Policies regarding Conditions of Employment up to and including termination.

IV. Supporting Documents

The following policies, administrative guidelines and forms are used in conjunction with this policy:

SAQ-PO-0460 – System Safety Policy

PS-PO-0110 Security & Emergency Preparedness Plan (SEPP)

IV.I Employee Standards of Conduct

IV.L Misuse of MARTA's Property

Metro Transit, Madison, Wisconsin

Security Camera Surveillance Police

49

Security Camera Surveillance Policy Metro Transit System

Objectives

The primary objective of having video surveillance is to document what transpires when events occur that threaten the safety of customers and/or employees of the transit system. The installation of cameras, with signage alerting customers and employees, has also been a deterrent to disruptive behavior and provides a sense of security to riders and employees. And finally, in case of personal injury accidents, a video record validates the facts.

Metro Transit has security surveillance cameras at the transfer points, on buses, and in our facility.

- All four Transfer Points are equipped with security cameras. Images are available in real-time via wireless connection to Metro staff and to the Madison Police Department.
- On-board video and audio surveillance equipment is installed on the entire fleet of fixed-route and paratransit buses.
- Cameras at Metro's facility monitor the cash-handling activities, document evening and weekend access to the Parts Room, and provide security for our employees at the building entrances and other public areas. In addition, there are exterior cameras providing security in the parking lot.
- There is signage in all locations providing notice that video (and audio on the buses) surveillance is present.

Downloading Images:

Digital video recorders store information. The hard drive is pulled and/or images downloaded when an incident is reported (by employees or the public). Otherwise, the hard drives are recorded over.

Access to Images:

- For safety and/or security incidents, the surveillance records are shared with individuals directly involved in investigating and following up on the incident. This includes Metro management staff, law enforcement officials, school officials, the City's insurance company, the bus operator, union officials, the offending individual (and his/her parents as appropriate), and others who may be directly involved in responding to the behavior.

Metro Transit Rules of Conduct call for police intervention, arrest and/or prosecution in situations in which an individual's actions present an imminent danger to the life or safety of him/herself or others, or to Metro property. Video evidence is particularly useful in enlisting police and prosecutorial support to enforce the policy in these emergency situations.

- Video images are also used to monitor ride loads, boarding activity, and other planning purposes. The Planning Manager has access to the video records for this purpose.
- The on-board video is also used for training purposes. The ability to develop training videos showing our own operators handling real life situations has been an excellent training tool. Metro Driver Instructors access the on-board video for this purpose.

Public Records:

- In consultation with the City Attorney's office and insurance company, Metro will maintain as a public record images downloaded from the recorders to Metro computers.
- In cases where follow-up action is taken, the images will become part of the files for the incident, and be maintained in accordance with relevant public records requirements.
- In cases of vehicular accidents, the images will be provided to our insurance company, who will maintain them as part of their case file in accordance with their record retention policies.
- The Transit Service Manager serves as the open records custodian for Metro Transit. This includes video surveillance tapes/records.

Updated January 15, 2009

Updated May 5, 2011

Updated December 17, 2012

Updated March 20, 2014

SUBJECT: USE OF SURVEILLANCE CAMERAS

Purpose: City of Madison agencies have identified a wide variety of legitimate business reasons to use surveillance cameras. The primary purpose of this policy is to protect the privacy rights of the public and the associational/collective action rights of City employees. This policy promotes security for the public and for City employees through timely surveillance of areas otherwise difficult to monitor.

Responsibilities:

Department of Information Technology (IT)

Shall design, acquire, manage and maintain the network infrastructure to support a City-wide enterprise surveillance camera system. IT shall, in accordance with APM 4-7 (Policy for the Procurement and Disposal of Electronic Products), assist agencies in obtaining surveillance systems that meets the agency's technical requirements and complies with the City's enterprise system technological standards and policies.

IT shall manage network connectivity issues, coordinate problem remediation, maintenance and replacement of devices connected to the enterprise camera system. Agencies that have their own IT and/or facilities maintenance staff capable of maintaining camera devices may provide their own maintenance and problem remediation support.

IT shall ensure that the enterprise camera system is capable of complying with all Wisconsin Public Records Laws for the capturing, retention and timely production of public records.

Department/Division Head Responsibility

City agencies may develop their own surveillance camera programs to address the security issues. However, agencies shall not purchase, create or maintain their own independent surveillance camera systems but rather they shall work with IT.

Department/Division Heads must adopt a written surveillance camera policy on the use of surveillance cameras. Such written policy shall be on file and available to the public for review with the City Clerk within 30 days of implementation of the surveillance camera system (See Common Council Resolution RES-08-00863). The policy must be reviewed by the IT Director, the City Attorney and the Human Resources Director prior to its implementation.

Owner Agencies

The authorized security contacts for owner agencies may grant access to their surveillance cameras for others outside the owner agency. The authority to manipulate the cameras will be restricted to owner agencies, unless otherwise specified by the owner agency. Others may be provided view only permissions to specified surveillance cameras by the owner agency. Owner agencies are responsible for determining whether there is potential evidence of a law violation that was captured by their surveillance cameras, generate a police case number, and complete the form requesting preservation of evidence.

Agencies must provide Information Technology with at least 30 days advance notice of their intent to purchase cameras in order to afford adequate time to provision the network infrastructure required to support the new devices.

Agency policies must address the following considerations:

- The circumstances which necessitate the use of surveillance cameras;
- Whether the agency will utilize the City's standardized enterprise camera system and if not, specify business/technical reasons prohibiting such use;
- The personnel, by name or position, that will have access to either the cameras or the data recorded by such cameras;

- The circumstances under which such personnel will have access to either the cameras and/or the recorded data;
- Whether the cameras will be recording video or both audio and video;
- The physical location of cameras and a description of the areas to be observed by such cameras;
- The corresponding location and the verbiage of signage alerting persons that their actions are subject to audio-visual recording. Such signage shall be conspicuous and shall clearly inform all persons that their actions are being both audibly and visually recorded;
- Unless otherwise prohibited by law, the Madison Police Department will be provided with immediate access to all data or recordings that may constitute evidence of a crime. The Madison Police Department shall determine, in consultation with the Dane County District Attorney's Office, whether to obtain a warrant to take custody of such data or recording;
- The time period that recorded audio/video will be retained and available. No retention period of less than fourteen days may be approved under this policy;
- Procedures for ensuring that records are not destroyed during the pendency of any public records request, investigation or civil/criminal litigation.

Every agency policy shall comply and each use of surveillance cameras shall comply with the Fourth Amendment to the United States Constitution and Article 1, Section 11 of the Wisconsin Constitution. Furthermore, agencies shall comply with the requirements of sec. 968.31, Wis. Stats. This requires close consultation with the Office of the City Attorney.


Each agency policy shall address any laws unique to that agency. For example, the Library's policy shall reflect consideration of sec. 43.30(5)(a), Wis. Stats. concerning the disclosure of library patron identities.

Every policy shall address the implications of any applicable collective bargaining agreement. Compliance with this provision requires close consultation with the Labor Relations Unit of Human Resources.

Agencies shall be responsible for the costs of procuring and operating the surveillance cameras they employ. Agencies shall use their budgeted funds to purchase all new camera devices, equipment, licenses, and services required to install and connect (fiber-optics, point-to-point radios, or any other network connectivity technologies) the devices to the enterprise camera system.

All enterprise cameras located in the street right-of-way will be owned by Traffic Engineering. Traffic Engineering shall provide maintenance and remediation support for cameras located in the street right-of-way.

Authority: Information Technology will interpret and maintain this APM.


Paul R. Soglin
Mayor

APM No. 3-17
December 13, 2012

Original APM dated 12/13/2012

Milwaukee County Transit System (MCTS), Milwaukee, Wisconsin

MCTS Employee Mobile Video Surveillance System (MVSS)
User Agreement

51

MCTS EMPLOYEE MVSS USER AGREEMENT

POLICY STATEMENT

The Milwaukee County Transit System (MCTS) has installed a new Apollo Mobile Video Surveillance System (MVSS) to ensure safety and security for our operators and passengers. Video from system can be used for any way that MCTS sees appropriate for the investigation and resolution of accidents, public or company complaints or commendations, performance or route issues or any security or safety issue.

It is the policy of MCTS to ensure the proper and appropriate utilization of the MVSS and to provide access of this expanded surveillance capability only to authorized staff. It is also the policy of MCTS that surveillance video captured by the MVSS will be used to assist with liability determination matters as they are brought to the attention of the MCTS Risk Management Department or other matters concerning MCTS interests. Users of the system have a responsibility to maintain integrity and confidentiality of all video stored on the system.

RSM SOFTWARE – LIVE LOOK IN AND ACCESS TO DVR

RSM software is primarily used to configure the DVR box on each bus as well as to resolve or diagnose any onboard issues. For the authorized end user, this software can also be used in a limited capacity to view all stored video on a hard drive/DVR, directly download clips or to view what is happening live on any bus in service from any MCTS workstation installed with RSM.

RSM is a very powerful tool, giving unprecedented access to live video of all buses in service. In order to preserve integrity of the system, address privacy concerns and control the use of the MCTS fixed and mobile networks, RSM access will be limited to specific persons during the project implementation and acceptance phase and a viewing station will be made available for users needing access to the system.

VIDEO SHARING POLICY

Sharing video or discussing MCTS video with an unauthorized person, viewing video unrelated to your direct work responsibilities, performing a secondary recording of MCTS MVSS video with a portable recording device or downloading MCTS MVSS video clips or still shots outside of the ViM software or the MCTS network is strictly forbidden and may be subject to discipline up to and including termination. Exceptions to this are videos released by authorized persons for police or legal investigations or through formally approved records requests.

I have read and understand the MCTS policy and accept the terms listed above ☐

Printed Name _____

Signature _____ Date _____

Monterey-Salinas Transit District (MST), Monterey, California

Memorandum to All Employees re Electronic Monitoring Systems

52



September 20, 2002

To: All Employees
From: Carl Sedoryk, Assistant General Manager
Subject: Electronic Monitoring Systems

In the interest of providing a safe and secure environment for our employees as well as our customers, Monterey-Salinas Transit has installed video cameras at the Wright Division, the Salinas Transit Center, on our new bus fleet, and various other MST locations. Additional video equipment may be installed at other MST locations based on continuing organizational and safety/security needs.

The purpose of the addition of video cameras at these and other locations is to help protect our employees, customers and property from threats of violence, and vandalism, regulate safety and security problems, and avoid sabotage and theft. Video surveillance will be limited to work areas and will not be placed in any private areas such as locker rooms, rest rooms and any area where an employee changes clothes. Audio recording will be added as a component of our communication system. The audio will affect all incoming/outgoing Communications Center radio and phone calls and emergencies associated with coach operator initiated covert alarms. Video cameras will be located onboard buses our new bus fleet (starting with 1701) at locations designed to monitor the safety and security of our employees, passengers and equipment.

Expectation of privacy

All employees of Monterey-Salinas Transit should understand that their communications through computer use and/or the Advanced Communications System are not automatically protected. For example, no messages should be sent using MST telecommunications equipment via text, voice, or radio should be considered private.

At any time and without prior notice, Monterey-Salinas Transit reserves the right to examine e-mail, personal file directories, and other information stored on MST systems. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of MST information systems.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

Please be advised that any monitoring-type equipment shall not be used in any manner that might potentially endanger the right of privacy or civil liberties of any individual. Should you have any questions, concerns or recommendations, please do not hesitate to contact me.

Re-Posted: February 3, 2004
File: February 13, 2004

To: All Coach Operators

From: Robert Weber, Operations Support Manager

Subject: Kal-A-Tel™ Video Surveillance System

The 1700, 1800, *new* 1100, and the 1900 (Trolleys) series coaches are equipped with the Kal-A-Tel™ Video Surveillance System. The system is equipped with four on-board (4) cameras, each of which is positioned to provide extensive surveillance of the interior of the coach. The surveillance system is for the most part, fully automatic. The system begins recording as soon as the coach's ignition switch is activated and will continue to record images for up to 30 minutes after the ignition switch has been turned off.

Located on the left rear panel of the 1700 and 1800 series coaches, is a button, (below), that once depressed, will allow you to flag a particular segment of the recording for easy retrieval, and increase the frame rate, which will enhance the overall clarity of the recording.



Please activate this feature whenever you observe any unusual, suspicious, or inappropriate behavior exhibited by your passengers. Once activated, the system will automatically flag that section of the recording and will begin recording the events at an increased frame rate for a five full minutes.

Should you have any additional questions concerning the use of the Kal-A-Tel™ system, please contact your supervisor.

STANDARD OPERATING PROCEDURE

Department:	Transportation
Version Number:	05
Approval Date:	10-29-2004
Revision Date:	07-29-2016

SEON Video Management, DVR Exchange, & Reporting Procedures

OBJECTIVE:

To establish guidelines to manage SEON Video / JPEG download(s), video review, and removal / replacement of SEON Digital Video Recording (DVR) systems.

PROCEDURE:

In order to assist with the investigation of incidents/accidents, or when video evidence is needed to determine specific chain of events, SEON request(s) for downloadable digital video recording shall be performed per the following guidelines

1. REQUESTS FOR SEON DOWNLOAD VIDEO OR JPG PHOTO(S):

- A. Safety and Risk Management or his / her designee shall be responsible for requesting download video from any Coach for any of the following reasons: (*Note: The list below is not intended to be all-inclusive*)

Vehicle Collisions:

- Involving all MST coaches.
- Involving any injuries including basic first aid, transporting an individual for emergency medical treatment, or resulting in a fatality.
- Resulting in disabling damage to any motor vehicle requiring tow.
- Resulting in extensive collision damage.
- Involving gross misjudgment or negligence.
- Unreported damage to MST vehicles or property

Other Incidents:

- Passenger falls (boarding/alighting or while on board) with reports of injury.
- Involving vehicle fires or the discharge of fire retardants.
- Involving the discharge of a weapon, or a physical altercation involving an assault between passengers or an MST employee.
- Involving any criminal investigation.
- After a report of a theft or robbery.
- Involving complaints of sexual harassment.

- B. Operations Supervisors or other Supervisory personnel shall be responsible for requesting SEON downloaded video for any of the following reasons:

- Customer complaints of inappropriate employee conduct.
- Reported violation of ADA regulations.
- Driving complaints
- Safety violations or reports of ongoing failure to observe MST policies and procedures.
- Immediate requests for video from law enforcement agencies or other public safety personnel.
- JPEG Photo's as needed for SETS (Service Exclusion Tracking System)
- Any other situation requiring video review.

2. SEON VIDEO REVIEW:

A. SEON video may be reviewed by the following staff as required:

- Risk & Security Manager, or designee, and Operation Supervisors: at any time to aid in the investigation of accidents or incidents; to determine if safety procedures were followed; or to assist in employee training.
- Risk & Security Manager, or designee: For any incidents or accidents involving a potential liability claim against MST; incidents involving potential criminal acts by passengers or employees.
- Managers / Supervisors: Incidents involving the report of unprofessional conduct by an Operator; accidents, improper driving complaints, or reported safety violations, which may require follow-up.
- GM/CEO, COO, and Department Directors: Any incidents involving a serious accident / incident, suspected criminal activity, or for any reason as requested.

3. REMOVING / REPLACING A SEON DVR(S):

A. Actual hard drive (DVR) pulls shall only be done for the following reasons :

- In the event an incident occurred where the video must be reviewed before the coach has pulled in the yard, or uploaded its GPS information.
- The bus has lost power and the video cannot be retrieved other than pulling the DVR.

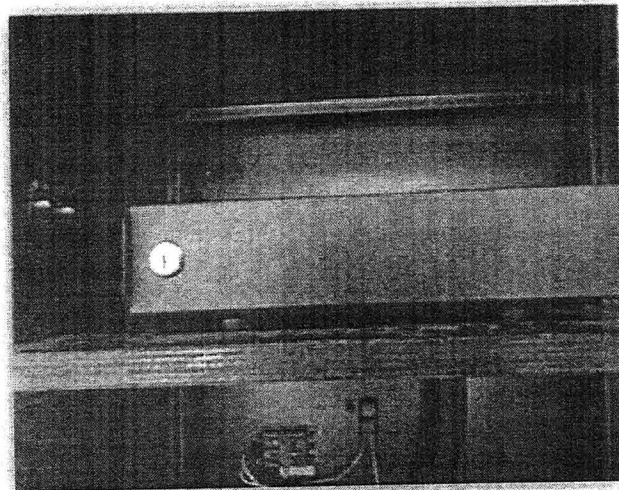
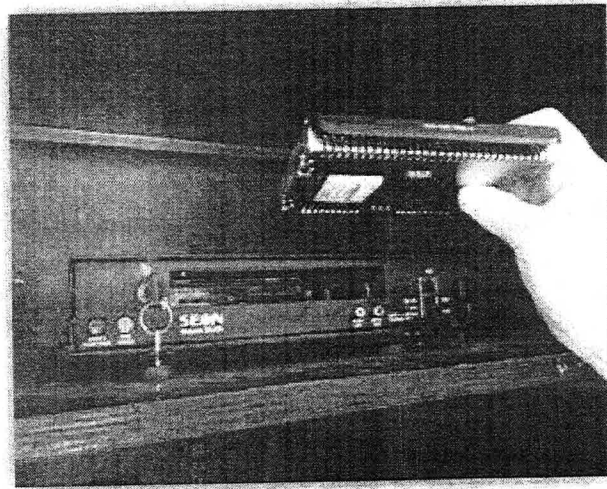
B. Hard Drive (DVR) pulls shall be approved in advance by the Safety and Risk Manager or his / her designee as follows:

- Communications, Supervisory, and other designated staff will coordinate the removal and replacement of a DVR unit. If an Operations Supervisor is not available to complete the exchange then a Maintenance Department Supervisor or designee will be contacted to pull the DVR unit.

C. DVR Removal:

- Unlock the DVR Cabinet with both the conventional key and the square "hex" key if the cabinet is so equipped.
- Unlock the DVR housing unit using the DVR key, remove the front panel and place to the side.
- Press the red button and wait for flashing red lights to stop.
- Use small round key to unlock the caddy.

- Slide the DVR out of the housing unit.




D DVR Replacement:


- Insert the replacement DVR unit.
- Make sure you use the round key to lock the caddy. If you fail to lock the unit it will not record.
- Place the front panel back on the unit and lock with a regular DVR key.
- Lock the DVR Cabinet with both the conventional key and the square "hex" key if the cabinet is so equipped.
- After about 30 seconds verify that the green LED light has illuminated on the Driver's Video Surveillance console. *In the event that the LED light fails to come on or is flashing green it means the cameras are not recording- repeat steps above if still not working report to IT immediately.*

4. SEON DVR REVIEW TAG & TRACKING RECEIPT:

- A. Prior to submitting any DVR for review, complete and affix, (with tape), a SEON DVR REVIEW TAG, (See below), to the front of the DVR. All required information shall be completed on the form prior to submitting the DVR for review.

 SEON <small>ACQUISITION</small>		
<u>SEON DVR REVIEW TAG</u>		
Reason For Exchange:		Routed To
<input type="checkbox"/> Collision	<input type="checkbox"/> Passenger Injury	<input type="checkbox"/> Maintenance Supervisor
<input type="checkbox"/> Customer Service Report	<input type="checkbox"/> Police Request	<input type="checkbox"/> Operations Supervisor
<input type="checkbox"/> Improper Driving Report	<input type="checkbox"/> Service Suspension	<input type="checkbox"/> Planning / Scheduling
<input type="checkbox"/> Medical Emergency	<input type="checkbox"/> NTD Route Survey	<input type="checkbox"/> Risk Manager
<input type="checkbox"/> Passenger Fall	<input type="checkbox"/> Unreported Damage	<input type="checkbox"/> Safety / Training Officer
<input type="checkbox"/> Passenger Disturbance	<input type="checkbox"/> Other	<input type="checkbox"/> Other
Date, Time, & Location of Incident: _____		
Incident Description: _____		
Coach #: _____ Employee Involved _____ EE#: _____		
DVR Requested By: _____		
(Detach & Affix to the SEON DVR)		

- B. Complete the SEON DVR TRACKING RECEIPT (See below) and forward it to the Director of Human Resources.

 SEON <small>ACQUISITION</small>	
<u>SEON DVR TRACKING RECEIPT</u>	
Coach #: _____ Date Pulled: ____/____/____ Time: _____ Pulled By: _____ (EE# / Last Name)	
DVR # OUT: <input style="width: 60px;" type="text"/>	DVR # IN: <input style="width: 60px;" type="text"/>
(Detach & Forward to Director of Human Resources)	

Pierce Transit, Lakewood, Washington

Task Outline, TSK-11200.11, Reporting Problems with Physical Security Equipment	55
---	----



TASK OUTLINE

Effective Date: June 29, 2009

Replaces: New

See Also:

Approved By: Joan Cormany, Manager of Physical Security & Records

TSK-1200.11 REPORTING PROBLEMS WITH PHYSICAL SECURITY EQUIPMENT

When a problem is observed on any system that is overseen by the Department of Public Safety, Physical Security and Records Division (CCTV, Limited Access, Alarm Systems, TOA Panic Alarms, etc.), the employee:

1. Notifies the Department of Public Safety Physical Security and Records Division of the problem by phone call or email
 - a. During normal business hours, 8 a.m. to 5 p.m. Monday through Friday (excluding holidays), call one of the following and give a detailed description of the problem
 - i. Manager of Physical Security & Records: 253-581-8090
 - ii. Transit Security Specialist: 253-983-2725
 - iii. Transit Security Specialist: 253-983-3424
 - b. Notification by email may be made at any time (Employee names and email addresses are listed in the current in-house telephone directory)
 - i. Provide as much detail in the email regarding the problem as possible
 - ii. Email will be reviewed the next regular business day
 - c. After business hours, (normal business hours are 8 a.m. to 5 p.m. Monday through Friday) contact the Communications Center @ 581-8109
 - i. The after-hours pager for Physical Security will be notified for all issues (Note: After hours notification is classified as anytime outside of Monday through Friday 8am to 5pm, to include weekends and holidays)
2. Notifies their direct supervisor or manager of the problem that was noted and that it was reported to the Physical Security & Records Division



POLICY

Effective Date: January 1, 2016 Review Due: January 1, 2017
Replaces: POL 1250.10 Cameras on Buses Sound Transit
See Also: Washington State Archives CORE Retention Schedule
Washington Courts' Rules of Evidence
Approved By: Executive Team

POL-1250.09 CAMERAS ON BUSES PIERCE TRANSIT

The purpose of this policy is to ensure proper handling of Agency mobile video cameras systems installed on rolling stock vehicles, including authorized use, storage, retention, maintenance and repairs.

Definitions

- a. AP/Access Point – the antennae which wirelessly retrieve the recordings from the vehicle.
- b. APC/Automated Passenger Counter – equipment which records passenger boardings and alightings.
- c. Authenticated Permanent Record – the final recorded record that is placed on a storage device for retention purposes. Serves as the Agency Master file.
- d. Authorized User – an Agency employee who is assigned and approved for the task of accessing, retrieving, archiving and/or disseminating authorized recorded records. The Office of Public Safety establishes authority levels.
- e. Chain of Custody – the chronological documentation of each person involved in the process of gathering a recorded record and making it an Authenticated Permanent Record, and the dissemination of authorized copies of that record and in any other manner having access to or possession of the recorded record.
- f. DVR – Digital Video Recorder, the on-board device which stores all imagery and audio recordings.
- g. Event – an event is created by way of an electronic 'flag' on the DVR when one of the following occurs: sudden braking, sudden swerving or turning or by use of the Event Button.
- h. Event Button – a button on the vehicle. At this time, the Event Button is not being used.
- i. Event-driven recorded records – When an event occurs, the flagged event-driven recording is automatically downloaded when a bus is in proximity to an access point. The recording is initially referred to as "non-criminal imagery." Depending on the circumstances, a given recording may change type during its archived status. Authorized Users should determine the current type designation when seeking use.
- j. FTA – Federal Transit Authority.
- k. Manually flagged event – events which are flagged manually by either contacting the Communications Center or by pressing the Event Button.

- l. Mobile Video Camera Recording – imagery and/or audio which is stored on the DVR.
- m. Mobile Video Camera Recorded Records– Imagery and/or audio records obtained from approved Agency equipment on board any rolling stock that is owned, leased or borrowed for Agency purposes.
- n. Prioritization Table – the table which defines the priority level and category or type of activities that fall under each level.
- o. Retention – the length of time a recording is retained.
- p. Requestor – the originator of any request for recorded records.
- q. Requestor Form – the form a requestor fills out when seeking approval to obtain a recorded record.
- r. Ride Check Verification Audit – an FTA requirement that transit agencies validate APC data by way of manually auditing randomly selected trips and comparing the data.
- s. Rolling Stock (as defined in Buy America regulations) - transit vehicles such as buses, vans, cars, railcars, locomotives, trolley cars and buses, and ferry boats, as well as vehicles used for support services.
- t. System Health Report – a report automatically generated by the wireless camera system and uploaded each time the vehicle is within range of an AP.
- u. Unauthorized duplication or dissemination – any use of imagery other than the intended or authorized use or use without official permission.
- v. Video Camera Recorded Record – All video or audio recordings from approved Agency Video Camera systems.

1. PURPOSE OF VIDEO CAMERAS ON AGENCY VEHICLES

Video cameras provide video and audio records which are used by the Agency to enhance customer service, crime prevention and detection and increase security and public safety efforts. These uses include but are not limited to:

- Responding to accident, incidents and/or public comment
- Prevention of acts of theft, vandalism, harassment and/or assault
- Identification of individuals involved in criminal activity on transit property
- Overseeing the safe daily operation of transit vehicles
- Assisting in law enforcement's investigation of criminal activity
- Deployment of Security and Law enforcement resources during events and emergencies
- Assisting Risk Management in the investigation and resolution of claims or complaints against the Agency
- As a training aid

2. MOBILE VIDEO RECORDING DEVICES WILL BE INSTALLED IN LOCATIONS WHERE THERE IS NO REASONABLE EXPECTATION OF PRIVACY

3. DISABLING OR DAMAGING VIDEO CAMERAS

- a. Employees are prohibited from disabling, damaging or otherwise rendering incapable any component(s) of the approved and installed camera system. Violations may result

in disciplinary action, up to and including termination and/or civil and criminal ramifications.

- b. Employees should contact the Communications Center immediately to report any acts of vandalism occurring in or on the vehicle.
- c. Only Authorized Users are allowed to manipulate the camera system. Authorized Users will be provided a level of access that meets the demands of their assignment only.

4. REQUESTING RECORDED RECORDS

- a. The Office of Public Safety will review and fulfill all requests for recorded records based on the Prioritization Table.
- b. All approved requestor forms will be responded to in an expeditious manner, typically acknowledging receipt of request within five (5) working days. All responses are to be in accordance with Agency policy and procedures as well as all State and Federal laws governing this type of request.
- c. All non-approved requests will be filed and notification will be sent to the requestor detailing the reason why the requested was denied.
- d. Responses to requests may be prioritized based on the legal requirements of the request. The Office of Public Safety maintains the Prioritization Table.
- e. Requests made by Union Leadership are handed in accordance with current Agency policy.
- f. Requests for Passenger Ride Check Audits will be generated by the Authorized member/s of Scheduling & Planning.

5. RESPONDING TO RECORDED RECORDS REQUESTS

- a. All requests for Recorded Records created or maintained for internal purposes such as Safety Review, Customer Service verification and complaint investigation or third party claims, are to be marked in such a manner to clearly identify the imagery media as "Non-criminal" and "For Official Use Only".
- b. All requests for Recorded Records created or maintained for criminal justice or law enforcement purposes are to be marked in such a manner to clearly identify the imagery media as "Criminal Evidence" or, if intelligence related as determined by Public Safety personnel, are to be marked "Law Enforcement Sensitive" or "LES". Criminal evidence or LES imagery will only be released to authorized recipients in accordance with State or Federal law.
- c. Employees in possession of non-criminal imagery are to treat the information as confidential and store such to prevent unauthorized use or duplication. Media containing imagery shall not leave the authorized user's possession while in use and shall be stored in an unobvious location in the user's office when not in use.
- d. All criminal evidence, SSI and LES will be handled and maintained in accordance with applicable Washington Courts' Rules of Evidence, court orders and Agency procedures.
- e. The Office of Public Safety will maintain a log of each request for Recorded Records and track the progress of each such request until the request has been closed. A thorough and documented Chain of Custody is to be maintained with each request. The Chain of Custody is maintained by the Office of Public Safety.

6. LIVE LOOK IN

- a. Live look in will only be permissible during a reported medical emergency, criminal or suspicious act or any other serious event that compromises the safety, security, and comfort of employees and customers onboard the bus. The employer will not randomly review audio or video data nor review it for the purpose of discovering policy violations in the absence of a precipitating event.
- b. Should a Supervisor, Security or Law Enforcement personnel witness an event occurring on the bus, they must call in the event and report what they witnessed **before** logging into Live Look In. They will be given the vehicle's credentials. Once a determination of the event is made, they must then call in again either confirming or clearing the event.
- c. Designated agency vehicles will be equipped with hardware allowing live look in inside a bus which is direct line of sight of the agency vehicle.
- d. Designated and trained personnel only will have credentials allowing them access to live look in.

7. USE OF RECORDED RECORD(S):

- a. All Users shall sign the CCTV Access Authorization form acknowledging they understand the Agency's policy on the use of electronic monitoring and recording systems.
- b. Physical or Uniformed Security will provide training for authorized users.
- c. Video Camera Recorded Records are for Agency Use Only and are always considered for official use only. Certain records may be designated either Security Sensitive Information (SSI) or Law Enforcement Sensitive (LES) or may be considered evidence in criminal proceedings or otherwise be subject to legal restrictions, e.g. litigation holds or other court orders.
- d. Unauthorized Access or Use of Agency Recorded Records may result in disciplinary action, up to and including termination, and/or civil and criminal ramifications.
- e. Any employee with knowledge of misuse of these systems is required to notify their supervisor immediately and provide facts and circumstances surrounding the misuse. The supervisor is to elevate the incident to the Office of Public Safety as soon as facts have been verified.
- f. Unauthorized duplication or dissemination of recorded record(s) is prohibited.
- g. Event-driven recorded records will not be reviewed unless a formal request is received.

8. PASSENGER RIDE CHECK VERIFICATION AUDIT

- a. Ride check verification audit videos will not be used for any other purpose unless one of the following is observed: illegal active, unsafe activity or activity that is against Agency policy and may be committed by either a member of the public or an Agency employee. If such activity is observed it shall be immediately reported to Public Safety for review.

9. RECORDED RECORDS HANDLING AND RETENTION

- a. Non-flagged and non-criminal records will be retained for a minimum of 30 days and then overwritten unless a Request form is received prior.
- b. Criminal records will be retained based on Washington State Archives CORE schedule. Currently this is 3 years.

10. MALFUNCTION

- a. The wireless camera system will produce a System Health Report which will be emailed to designated Fleet Maintenance and Public Safety for review.
- b. Each vehicle equipped with a camera system, wireless or hard drive, has an indicator light which alerts the Operator of a malfunction.
- c. Employees shall report all nonfunctional or damaged equipment as soon as practical, but no later than the end of shift.
- d. Malfunctions shall be reviewed by Fleet Maintenance and repaired as soon as practical.
- e. The Communications Center will determine whether a bus change is needed.

11. MAINTENANCE AND OPERABILITY

- a. The Department of Public Safety is responsible for the use and maintenance of the CCTV and recording systems for fixed systems.
- b. Fleet Maintenance is responsible for the operability and maintenance of electronic monitoring systems on rolling stock.

Prioritization table attached here for reference only.



DEPARTMENT OF PUBLIC SAFETY



FIXED & MOBILE CCTV REQUESTS

The project and system are monitored live at Tacoma Dome Station by our Public Safety Officers. Over the years, we have developed a process to securely deliver this video imagery when requested and have an established protocol for chain of custody.

In July 2013, thirty of the Sound Transit fleet were equipped with CCTV that also captures audio. The ST system did not include supporting infrastructure thus requiring all requested video to be removed manually in the event of a request. What this means is that requests for ST video will be a time consuming process and in most cases will be completed here at the base so as to minimize service disruption and maintain recorder integrity.

The Office of Public Safety has been tasked with developing the process for collecting and tracking all CCTV requests, fixed and mobile, as well as establishing the accountability procedures and chain of custody. In order for us to provide this service timely, I wanted to lay out the procedure for you on how you go about getting video if needed.

The CCTV request form has been developed to assist you with your requests and also serves as part of our tracking system. We consider all management as authorized requesters and will only initiate the collection process with this form coming from an authorized requester. Please provide as much of the information as possible to assist us with narrowing down the time frame of the video request, again with the ST mobile system, it has to be completed manually. Each of the approved requests will be prioritized as indicated on the form. The below table is our initial goals for turnaround time with all approved requests:

PRIORITY TABLE

Priority (1)

Turnaround time: within 24 hours

- Major Crimes Against Persons
- Fatal Injury Accidents
- Major Events (Unclassified)
- Tempering/Vandalism of CCTV System

***On Call Duty Officers are to be notified of Priority (1) requests

Urgent (2)

Turnaround time: within 72 hours

- Serious Injury Accidents
- Serious Incidents
- LE or Prosecutor Requests
- All Incarceration Arrests



- Time Sensitive/Retention Sensitive
- Alleged Criminal Employee Misconduct
- Use of Force

Routine (3)

Turnaround time: within 10 business days

- All Other Arrests
- All Other Accidents
- PDRs
- Alleged Non-Criminal Employee Misconduct
- Property Damage
- Internal Agency Requests
- Other Requests No Qualifying as Priority 1 or 2

This form is intended for *Internal Use Only*. Once you have completed the form, save a copy for yourself. Send the form, via e-mail, to the "CCTV Request Desk." You will then receive a response from Public Safety Records letting you know that it has been received and what priority code it has been assigned. Once your requested video is complete you will be notified and a copy will be provided to you upon signing the chain of custody form.

***NOTE: As a holder of a video record, you will be responsible for the security of that record as well as the destruction of it according to the Washington State Retention Schedule. A retention schedule will be provided at a later date. Future plans are to place the request form on IPT with a memo outlining the procedure for all employees.

As with all procedures, they are subject to change. We are not sure yet how well this process will work; however, your patience as we continue to refine this process will be greatly appreciated.



Rhode Island Public Transit Authority, Providence, Rhode Island

Rhode Island Public Transit Authority Administrative Policies and
Procedures, Surveillance Camera Policy

58



The Rhode Island Public Transit Authority
Administrative Policies and Procedures
Office of the Chief Executive Officer

Subject/Title Surveillance Camera Policy	Effective Date: _____, 2014 Supersedes:
	Approval: CEO

I. PURPOSE

RIPTA has determined that the use of surveillance cameras and surveillance recordings at RIPTA facilities and on RIPTA vehicles is necessary to ensure the safety and security of all RIPTA employees, visitors, riders, vendors, property and equipment. Such use will improve safety and security by deterring acts of theft, violence and other criminal activity, and will increase the likelihood that perpetrators of these acts will be identified. Such use will also permit the monitoring of activity that may cause property damage or personal injury, and will assist RIPTA in carrying out its daily operations. RIPTA has created this policy in furtherance of these purposes.

II. SCOPE

This policy applies to all RIPTA employees, visitors, riders, contractors, facilities and vehicles.

III. CAMERA LOCATIONS

1. Surveillance camera will be installed in all RIPTA facilities and fixed route and Ride/Flex vehicles. Areas subject to surveillance will be identified by signs posted at the entrance to the facilities and vehicles. By entering the areas subject to surveillance, individuals will consent to being observed and/or recorded by the surveillance cameras present.

2. In accordance with Rhode Island General Laws Section 28-6.12-1, no video recording will be made of a RIPTA employee in a restroom, locker room, or room designated by RIPTA for employees to change their clothes, unless authorized by court order.

IV. USE AND RETENTION

1. Surveillance cameras and recordings shall be used by RIPTA in furtherance of the purposes of this policy. In the event of an incident that implicates the purposes of this policy, a surveillance recording may be used to assist in the investigation of the incident and may be provided to law enforcement personnel.

2. Unless otherwise required by law or court order, recordings from the surveillance system will be kept for a period of time chosen by the Chief Executive Officer or his/her designee.

3. Unless required by law, subpoena, or court order, only the Chief Executive Officer and designated personnel from RIPTA's Security, Claims, Legal, Human Resources, and Transportation and Maintenance Departments may request or view recordings from RIPTA facilities or vehicles. However, the Chief Executive Officer or his or her designee may authorize additional personnel to access the recordings if doing so would further the purposes of this policy.

V. *DESTRUCTION or TAMPERING WITH EQUIPMENT*

1. Any RIPTA employee, who destroys, alters the image of, interferes with the operation of or otherwise tampers with a video camera or any part of the video surveillance system will be subject to disciplinary action and may be subject to prosecution in the criminal justice system.

2. Any RIPTA employee who fails to follow this policy or who willfully damages any surveillance equipment will be subject to disciplinary sanctions, up to and including termination.

DESCRIPTION OF RECORDS**RIPTA RETENTION POLICY****RISK MANAGEMENT**

Workers Compensation Records	Retain for 10 years (in case of reoccurrence), then discard.
Liability / Claim Files	Retain for 7 years, then discard.
Insurance Policies	Retain for 3 years after policy expires (the statute of limitations for filing a claim); then discard.

SAFETY & SECURITY

Hazardous Materials Manifests	Retain a minimum of 3 years per RCRA. RIPTA keeps permanently.
Land Ban Restriction Records	Retain a minimum of 5 years, per EPA.
Material Safety Data Sheets	Retain for 30 years, then discard.
Right to Know Training Records	Retain in employee personnel files.
Hazwoper Training Records	Retain in employee personnel files.
RCRA Training Records	Retain in employee personnel files.
Safety Department Inspections (internal)	Retain a minimum of 1 year per EPA.
Spill Prevention Control & Countermeasure Plan (SPCC)	Retain a minimum of 7 years.
Electronic Surveillance Files	Retained at the discretion of Director of Safety, CFO and General Manager.
OSHA 300 Forms (worker injury)	Retain a minimum of 3 years; RIPTA retains permanently.
Incident Reports / Operator Safety Records	Retain for current employees + 3 years.
EPA/RI DEM Air Emission Files	RIPTA retains permanently.

MAINTENANCE

Building Blueprints	Retain until superceded, then discard.
Vehicle Maintenance Records	Retain records for 3 years after: a) the end of useful life, or b) asset is sold; or c) asset is disposed of; then discard.
Maintenance Records for Equipment & Non-Vehicle Assets	Retain records for 3 years after asset is sold, replaced or disposed of; then discard.
Safety / Housekeeping Inspection Reports	Retain records for 3 years, then discard at discretion of AGM Maintenance.
Third Party Inspection Records	Retain records for 3 years, then discard at discretion of AGM Maintenance.

PLANNING

Real Property Records	Retain for 3 years after interest in property is sold or transferred.
Real Property Inventory & Plans	Retain until superceded.
Ridership Records & Estimates	Retain for a minimum of 7 years.
Scheduling / Bus Routing Records.	Retain for a minimum of 3 years.
Reports, Analyses and Project Development Documents	Retain as determined useful to serve as supporting documents for future project development.

TRANSPORTATION

Personnel Files & Training Records	Retain in department for active employees; forward to Human Resources upon transfer, retirement or termination.
Incident Reports / Driver Safety Records	Retain in personnel files and Safety Department files.
Drug & Alcohol Testing	Retain records 1 to 5 years, per FTA requirements.

SPECIALIZED TRANSPORTATION

Personnel Files & Training Records	Retain in department for active employees; forward to Human Resources upon transfer, retirement or termination.
Incident Reports / Driver Safety Records	Retain in HR personnel files and Safety Department files.
Drug & Alcohol Testing	Retain records 1 to 5 years, per FTA requirements.

INFORMATION TECHNOLOGY

AS400 Computer System	Monthly Back-ups retained permanently.
Wide Area PC Network	Monthly Back-ups retained permanently.

CCTV MONITORING & PRESERVED FOOTAGE POLICY	POLICY	
	Document Number:	SSS-SE-PL-0001
	Version Number:	01

1.0 Purpose:

Santa Clara Valley Transportation Authority ("VTA") uses Closed Circuit Television (CCTV) to monitor its premises, bus and light rail vehicles, as well as light rail platforms to provide for the security and safety of its staff and the public and conduct its business. This Policy will serve as guidance to VTA for the use of CCTV security systems and outline responsibilities of respective staff when handling and utilizing CCTV Footage.

2.0 Scope:

This Policy applies to VTA Board Members and employees, as well as any VTA consultants, contractors and agents with respect to the use and monitoring of CCTV Footage.

3.0 Responsibilities:

- 3.1 System Safety & Security Management is responsible for providing safeguards for personnel with access to CCTV systems and Footage, authorizing access to CCTV systems, and ensuring that the CCTV systems are used in accordance with this Policy.
- 3.2 Protective Services is responsible for overseeing the CCTV systems and coordinating the use of CCTV monitoring and recording for safety, security and business purposes at VTA.
- 3.3 The Office of the General Counsel is responsible for responding to California Public Records Act requests and other requests pursuant to law.
- 3.4 Division Supervisors and Superintendents are responsible for authorizing the review of CCTV Footage for safety, security and/or business purposes.

4.0 Policy:

4.1 CCTV Monitoring

VTA will comply with state and federal law in the monitoring and treatment of CCTV Footage. Additionally, CCTV monitoring and recording shall be conducted in accordance with all existing VTA policies, including the non-discrimination policy, sexual harassment policy and other relevant policies.

<i>CCTV MONITORING & PRESERVED FOOTAGE POLICY</i>	POLICY	
	Document Number:	SSS-SE-PL-0001
	Version Number:	01

Legitimate safety, security and business purposes for CCTV monitoring include, but are not limited to the following:

- a. Protection of persons, property and buildings (e.g., may include things such as building perimeter, entrances and exits, lobbies and corridors, receiving docks, buses, light rail trains, light rail platforms, etc.);
- b. Video surveillance of public areas (e.g., parking lots and facilities, transit stops, streets and ways, commercial areas, public gatherings, etc.);
- c. Criminal investigations (e.g., robbery, burglary, theft, etc.);
- d. Protection of pedestrians (e.g., pedestrian and vehicle traffic activity, etc.); and
- e. Investigations (i.e. disciplinary, accident, customer complaint, criminal, etc.);
- f. Legal holds; and
- g. Any purpose that serves VTA's business needs.

VTA will maintain a secure database of all VTA owned and controlled camera locations and provide signage to indicate the presence of CCTV cameras where appropriate. Monitoring and use of Footage shall be conducted in a manner that properly balances VTA's legitimate safety, security and/or business purposes with the public's reasonable expectation to privacy.

When authorized employees are viewing Footage on a video monitor, the monitor will be in a position that cannot be viewed by others.

4.2 Preservation of Recorded CCTV Footage

CCTV Footage may only be preserved in connection to one or more of the purposes defined in Section 4.1 of this Policy. Unless existing Footage is preserved, new Footage will be captured over the previous Footage. The availability of non-Preserved Footage shall generally not exceed 30 calendar days.

<i>CCTV MONITORING & PRESERVED FOOTAGE POLICY</i>	POLICY	
	Document Number:	SSS-SE-PL-0001
	Version Number:	01

4.3 Requests for CCTV Footage

4.3.1 Law Enforcement Requests

VTA will provide local law enforcement agencies with CCTV Footage upon request in connection with any ongoing criminal investigation, as required by law.

When requesting Footage from VTA, local law enforcement agencies are required to submit the request in the form similar to the attached **CCTV Data Release Form** for approval and record keeping purposes.

4.3.2 Requests from VTA Staff for Legitimate Business Reasons

A supervisor or superintendent's authorization is required before VTA staff may use CCTV Footage to conduct an investigation (e.g. disciplinary, customer complaint, accident/incident, etc.).

4.3.3 California Public Records Act (CPRA) Requests of Footage

Outside of the aforementioned categories, CCTV Footage may be subject to the CPRA in a variety of contexts. Any request for CCTV Footage that is unrelated to a law enforcement matter or VTA's business reasons, will be referred directly to the General Counsel's Office for response and processing.

4.3.4 Subpoenas

Subpoenas and any other requests made pursuant to law must be directed to the General Counsel's Office for response and processing.

4.4 Reporting to VTA's Board of Directors

VTA staff shall provide an annual report to the Board of Directors at the end of any calendar year where Footage is preserved pursuant to section 4.1(g) of this Policy. The report shall include a description of the Preserved Footage, the identity of the requesting staff, the date of when the request was made and a statement articulating VTA's business need for the Footage.

<i>CCTV MONITORING & PRESERVED FOOTAGE POLICY</i>	POLICY	
	Document Number:	SSS-SE-PL-0001
	Version Number:	01

4.5 Retention of Preserved CCTV Footage

Except Footage specifically awaiting review by local law enforcement agencies, where a legal hold has been placed on the Footage or where staff has articulated that the Footage is required for a legitimate business reason, all Preserved Footage shall be destroyed in accordance with VTA's Record Retention Schedule, Policy and Procedure. The retention schedule pertaining to Preserved Footage captured by VTA's CCTV program is also attached herein.

4.6 Misuse of CCTV Footage

Any interception, duplication, transmission, diversion, or use of Footage and CCTV technologies for purposes other than the legitimate safety, security, and/or business purposes contemplated by this Policy is prohibited. Violation of this Policy may result in disciplinary action consistent with VTA's rules and regulations.

5.0 Definitions:

- 5.1*** "Closed Circuit Television" (CCTV) is a generic term used to describe a variety of video surveillance technologies. More specifically, CCTV refers to a system in which one or more video cameras are connected in a closed circuit or loop, with the images produced being sent to a central television monitor or recorded.
- 5.2*** "Footage" refers to video recording captured by VTA's CCTV system. Such video recordings are generally deleted after 30-days unless they are preserved (*see* Sec. 5.3-"Preserved Footage.")
- 5.3*** "Preserved Footage" refers to video recording that is downloaded and stored.
- 5.4*** "Reasonable Expectation of Privacy" is an element of privacy law that determines in which places and in which activities a person has a legal right to privacy (e.g. in a home, personal automobile, etc.).


6.0 Summary of Changes:

Initial release of this Policy.

Original Date:	Revision Date:	Page 4 of 5
04/7/2016		

CCTV MONITORING & PRESERVED FOOTAGE POLICY	POLICY	
	Document Number:	SSS-SE-PL-0001
	Version Number:	01

7.0 Approval Information:

<i>Prepared by</i>	<i>Approved by</i>
 Robert Fabela General Counsel	April 7, 2016 see attached certified copy Board of Directors

Original Date:	Revision Date:	Page 5 of 5
04/7/2016		

SANTA CLARA VALLEY TRANSPORTATION AUTHORITY

**REQUEST OF LAW ENFORCEMENT AGENCY FOR RELEASE
OF RECORDED AUDIO/VIDEO DATA**

1. DATE OF REQUEST:
2. DESCRIPTION OF INCIDENT LEADING TO REQUEST:

Date:

Time:

Location:
3. REQUESTING LAW ENFORCEMENT AGENCY:
4. CASE/EVENT NUMBER(S):

5. CERTIFICATION OF OFFICER:

On behalf of the above-named law enforcement agency, the undersigned officer has requested from Santa Clara Valley Transportation Authority (VTA) a copy or copies of available video and audio data related to the incident described above. I certify that this incident is subject to an official investigation by my law enforcement agency and that the copied video and audio data and any reproductions of any kind made from the video will be used for no other purpose than to assist in that investigation. *It is understood and agreed that the recorded video and audio data and all reproductions made from the video will remain the property of VTA and shall not be copied or released to anyone without VTA's General Counsel's prior written authority. Please contact 1-408-321-7581.*

My law enforcement agency agrees to indemnify VTA for any damage or injury that may arise from the unauthorized use or release of the recorded video and audio data.

The above-named law enforcement agency understands that VTA, as a public agency, is subject to the California Public Records Act (CPRA).

By: _____
Print Name:
(Sign above and include rank, badge number and contact number of requesting officer.)

RELEASE OF AUDIO/VIDEO DATA TO LAW ENFORCEMENT AGENCY

On _____ at approximately _____ hrs., I released to the officer identified above a copy or copies of the following recorded video and audio data:

DATE OF INCIDENT	CAR/TRAIN NUMBERS	BUS/BLOCK NUMBERS	LRT STATION TRANSIT CENTER or FACILITY	TIMEFRAME

By: _____

Print Name:

(Sign above and include title and extension of authorized VTA staff member.)

REFUSAL TO RELEASE AUDIO/VIDEO DATA TO LAW ENFORCEMENT AGENCY

On _____ at approximately _____ hours, I refused to release a copy or copies of the requested audio/video data to the officer identified above for the following reason(s):

By: _____

Print Name:

(Sign above and include title and extension of authorized VTA staff member.)///



Date: March 21, 2016
 Current Meeting: April 7, 2016
 Board Meeting: April 7, 2016

BOARD MEMORANDUM

TO: Santa Clara Valley Transportation Authority
 Board of Directors

THROUGH: General Manager, Nuria I. Fernandez

FROM: Director of System Safety & Security, Steven Keller

SUBJECT: Closed-Circuit Television (CCTV) Policy

APPROVED ACCEPTED ADOPTED AMENDED DEFERRED REVIEWED
 Santa Clara Valley Transportation Authority
 Board of Directors
 Elaine F. Baltes, Board Secretary
 BY: *Theresa Young*
 DATE: 4/7/16

Policy-Related Action: Yes

Government Code Section 84308 Applies: No

ACTION ITEM

RECOMMENDATION:

Review and adopt the CCTV Monitoring & Preserved Footage Policy.

BACKGROUND

Public agencies across the state of California have increasingly implemented Closed-Circuit Television (CCTV) systems for safety, security and business purposes. Public transportation agencies have placed cameras strategically in the interior and exterior of agency buses, light rail vehicles, facilities, property and platforms. The ability to monitor and preserve footage when necessary has been instrumental in deterring crime as well as aiding in criminal, disciplinary and risk management fact-finding investigations.

Public agencies such as Los Angeles County Metropolitan Transportation Authority (LA Metro), San Francisco Municipal Railway (SF Muni) and Sacramento Regional Transit (SacRT) have developed protocols for the handling of CCTV footage, including but not limited to requiring law enforcement agencies to submit formal requests for video, dealing with public record requests on a case-by-case basis and requiring supervisory approval of the respective department for video requested for a legitimate business reason. Presently, VTA staff follows similar protocols for the handling of CCTV footage and with Board approval will establish a policy formalizing these protocols.

CERTIFIED COPY

DISCUSSION:

The Policy will be applicable to VTA Board Members, divisions and employees, as well as any VTA consultants, contractors and agents with respect to the monitoring and use of video footage collected from CCTV systems on VTA's buses, trains, platforms and premises. In addition, the Policy will set forth responsibilities for System Safety & Security, Protective Services, the Office of the General Counsel and Division Supervisors and Superintendents. Protective Services within System Safety & Security will be the monitoring and record-keeping division for the CCTV system and footage.

The Policy will ensure that VTA complies with state and federal law in the monitoring and treatment of CCTV footage as well as remain compliant with its own policies, including the non-discrimination policy, sexual harassment policy and other relevant policies.

The Policy will set forth that VTA shall use its CCTV system only for legitimate safety, security and business purposes and provide the following delineated list for VTA staff as guidance for what purposes CCTV monitoring may take place:

- Protection of persons, property and buildings;
- Video of public areas;
- Criminal investigations;
- Protection of pedestrians;
- Investigations;
- Legal holds; and
- Any purpose that serves VTA's business needs.

By providing the above-referenced list, VTA will balance VTA's concern for security and safety as well as legitimate business needs with the public's reasonable expectation of privacy. As such, VTA presently provides signage on light rail trains, buses and stations informing the public of the possible presence of CCTV cameras, and will continue to do so. Although not required by law, the posting of signage has been a common practice of many public transportation agencies throughout the state of California and the Country.

VTA's CCTV system is set up in such a way that unless footage is preserved ("downloaded") for one of the purposes listed above, new footage will override the previous footage approximately every three weeks, depending on the age of the equipment in place. The Policy will provide that the availability of unpreserved footage (footage not downloaded from the CCTV system) will generally not exceed 30 days. The purpose of this provision is to avoid unnecessary monitoring and preservation of miscellaneous footage that does not serve one of the legitimate purposes for which VTA implemented the CCTV system. Footage preserved for legitimate purposes will be destroyed in accordance with VTA's Record Retention Schedule, Policy and Procedure.

CERTIFIED COPY

Accordingly, the Policy will provide guidance to VTA concerning requests for footage and how the footage should be handled. For example, the Policy will allow law enforcement agencies to request footage by submitting a CCTV Data Release Form. Being that time is crucial to criminal investigations, the goal here is to allow law enforcement agencies to request and view video footage in an efficient manner, without additional obstacles that may delay an investigation, but to nonetheless require certain standards to be met, as monitored by VTA. Requests from internal VTA staff will need to come from a supervisor or superintendent as to identify a proper business reason. The General Counsel's Office will oversee requests made under the California Public Records Act on a case-by-case basis and determine whether the public interest served by not disclosing the footage outweighs the public interest served by disclosure of the footage. In addition, staff shall direct all other requests made pursuant to law to the General Counsel's office for response and processing.

Lastly, the Policy will allow System Safety & Security management to make decisions regarding the CCTV technology and safeguards for handling of that technology so that VTA may continue to prioritize the safety and security of the public as well as the best interests of VTA.

FISCAL IMPACT:

No fiscal impact as a result of this action.

STANDING COMMITTEE DISCUSSION/RECOMMENDATION:

This item was reviewed at Administration & Finance Committee on March 17, 2016. Present was Board Chair Baker, Vice Chair Nguyen, Member Chavez, and Alternate Member Carr. The Committee was supportive of this policy. Board and Committee Member Chavez made the following request:

- Staff reference and attach the VTA records retention Policy.
- Staff embed this policy into any VTA policy and practices relating to how VTA manages and maintains data.
- Staff consider including this policy as appropriate in procurement packages so that vendors understand VTA's privacy needs.
- Staff provide an annual report to the Board of Directors in any calendar year that CCTV video is captured or used as outlined in CCTV Monitoring & Preservation Policy section 4.1 under the bullet point which reads: "Any purpose that serves VTA's business needs."

Prepared by: Steve Keller, Director of System Safety & Security
Memo No. 5476

ATTACHMENTS:

- UPDATED CCTV POLICY (FINAL) (PDF)
- Retention Policy - Protective Service_FINAL_02 12 2016 (PDF)

I certify that the foregoing instrument is a true and exact copy of the original on file in the Secretary of the Board of Director's office.

Date

Glaire Par
4/8/16

Tri-Met, Portland, Oregon

Tri-Met Security re Camera Installation/Change Request

62

TRIMET SECURITY	
Fixed : Camera Installation/Change Request (Fixed Facilities)	SEC401 SSE-612
Date: 10/16/14	Page 1 of 3

1.0 Purpose:

These procedures outline the process for requesting new security camera installations, home view state changes to existing Pan/Tilt/Zoom (PTZ) capable cameras or changing existing location configuration for all TriMet Closed Circuit Television (CCTV) cameras on TriMet Property.

This does not include Vehicle Borne CCTV, Office Communication Video Equipment or cameras used for training purposes.

Cameras will not be installed without a complete camera installation/change request form.

2.0 Procedures:

1. Complete the Camera Installation/Change Request Form (see below) with as much detail as possible. Make sure to include a contact phone number so that the CCTV Coordinator can reach you with any questions.
2. If you want to change an existing camera PTZ home view state, submit the camera name and an example of where you want it focused.
3. For new camera installations, submit a detailed description, drawing and/or photos of the location and proposed camera view(s). State whether this installation/change request is permanent or temporary, and if temporary, include the date this camera is no longer needed.
4. List all users that will need access to the proposed camera installation or change.
5. Submit the form to the Security Department, TPD Attn: CCTV Coordinator for processing along with a picture or map showing where cameras are to be installed and direction of you would like camera pointed. The following is the processing procedure:
 - 5.1 The completed form will then be returned to the CCTV Coordinator and it will be reviewed to make sure all information needed has been included, if not the CCTV Coordinator will make necessary phone calls to the requestor to obtain additional information so that the form can be completed correctly;
 - 5.2 If the form has been completed properly the CCTV Coordinator will submit the form to the Executive Director of Safety, Security, and Environmental for signature and approval;
 - 5.3 If approved by the Executive Director, the form will be faxed by the CCTV Coordinator to the Systems Engineer to begin the process for camera installation based upon the information received;
 - 5.3.1 If the form is not approved, the requestor will be notified by the CCTV Coordinator why the request was denied and further discussions between the CCTV Coordinator, requestor and Executive Director can be arranged to go over any issues;
 - 5.4 System Engineer will inform CCTV Coordinator that camera(s) have been installed;

CAMERA INSTALLATION/CHANGE REQUEST FORM

Date of Request: _____ Date Received
by Security Department: _____

REQUESTER: Name: _____
Department: _____
Phone Number: _____

Existing Camera: Y / N If Yes, Camera Name _____

New Camera: Location (attach area drawing/photos of location)

Permanent or Temporary Installation _____ If Temporary, End Date: _____
Business Need: _____

Account Number to be charged: _____

Approved By: _____ Approval Date: _____

Safety and Security Executive

=====

WORK ORDER:

Routed to: _____

Instructions/Notes: _____

Date Completed: _____

Approved By:
Manager Technical Services: _____
Supervisor MOW Communications: _____
Engineer IV Communications: _____

Nextiva Access Granted: _____

TRIMET SECURITY	
Fixed: CCTV Camera Acceptance (Fixed Facilities)	SEC102SSE-613
Date: 10/16/14	Page 1 of 2

1.0 Purpose:

This procedure describes the process for accepting cameras in the Closed Circuit Television (CCTV) Video Management System Software.

2.0 Departmental Procedures:

Cameras and other CCTV end-point devices must undergo testing and tuning before they will be accepted and are considered "in-production." After acceptance, these devices will be made available to the user community of the CCTV System.

1. Request Camera:

Request camera and provide information on install location, who needs access, by Submitting a Camera Access Request Form to Executive Director of Safety, Security and Environmental per SOP SEC101.

2. Reserving Camera in Solarwinds:

Capital Projects coordinates with IT CCTV Systems Engineer and enters camera details and reserves an entry into Solarwinds. IT will then assign IP Addresses for cameras to be installed in the field.

3. Setup Installation:

Certain information about the camera or other device must be known before other actions can be taken, such as camera naming, numbering, map creation, and import into video management systems. Initial setup is coordinated between the initial installer, CCTV System Coordinator and the CCTV Systems Engineer. The required information includes:

- Network Information: MAC Address, IP Address, Admin Password, pan/tilt/zoom (PTZ) configuration, and screenshot of homestate.
- Camera general location: Platform, or facility name.
- Camera specific location: Map or GPS coordinates.
- Camera name: Based on naming convention (See attached "Camera Naming Convention").
- Camera View: Security and requesting Department will determine camera view.

4. Installing Camera in the Field:

Before a camera may be accepted, the following areas must be tested in the test video management system. CCTV System Coordinator and CCTV Systems Engineer will test camera in video management system.

- Network connectivity and throughput.
- Recorded footage availability.
- Camera view is correct.
- The least amount of pixilation, ghosting and/or compression artifacts must be applied to the camera if the default configuration is not acceptable.
- If a PTZ, the camera's home setting must be configured.
- The camera's day/night setting must be adjusted if the default is not acceptable.
- The camera's settings of contrast, brightness or other picture quality settings must be configured if the default is not acceptable.

5. Video Management:

Camera is imported into the Video Management System and placed in station folder, where only administrators and those involved in testing/tuning may access it by the CCTV Systems Engineer. Folder is same location as final location, but the camera(s) are not visible until accepted for service.

- a. Camera is tested, tuned, and viewed with Security for approval of the camera for use by Users.
 - b. The camera(s) are now considered in production and available for CCTV customer use.
- 6. Camera Monitoring in Solarwinds:**
Camera monitoring via SNMP must be enabled so that automated alerts can be dispatched when camera is in fault state.
- 7. Camera Acceptance:**
Once camera passes acceptance procedure, Security makes camera visible to appropriate users and camera is considered "In Service".

Additional CCTV References:

SEC101-SSE-612 – CCTV Camera Installation/Change Request (Fixed Facilities)
SEC103-SSE-614 – CCTV Video Management System User Access (Fixed Facilities)
SEC104-SSE-615 – CCTV Roles and Responsibilities
 HR Policy 207.1 – Information Technology CCTV Use

CAMERA NAMING CONVENTION

Sample: 188EB04-EEndShelterNWLkgE-IN1

Rockwood/188th - EB - 04 - East End of Platform, NW Corner under Shelter, Looking East, Encoder Input 1

Location	3 Char	CLE-Cleveland, 188-Rockwood/188th, CIV-Civic, etc.
Direction (Platform)	2 or 3 Digit	EB, WB, CTR, etc. (CTR would apply to locations where the platform is between the rails and/or services multiple directions)
Camera Number	2 Digit	01, 02, 03, etc. (EB/WB platform cameras should be numbered grouping them together)
Details of Location the cameras is mounted on the platform and the cameras view		EEndMPLkgW (East end of Platform, mounted on Map Pylon, Looking West) No need for the words Platform, Park-n-Ride, etc., Use Mid for cameras that are mounted on something in the middle of the platform)
Encoder Input # (Analog Only)	IN__	IN1 - Input 1 on the encoder

TRIMET SECURITY	
Title: CCTV Video Management System User Access (Fixed Facilities)	SEC103SSE- 614
Date: 10/16/14	Page 1 of 1

1.0 Purpose:

This procedure describes the granted rights of Closed Circuit Television (CCTV) Video Management System (VMS) Users.

2.0 Procedures:

- Users in the CCTV VMS are granted rights as part of their membership in groups. No rights are specifically assigned to an individual user.
- Users may be part of multiple groups. Permissions are an aggregate of the groups' permissions to which they belong.
- Groups will be primarily used to separate users' camera accesses: Nextiva Groups will have a "role-based" permission applied to them which may mirror other groups' "use" permissions.
- CCTV VMS User Permission Types:
 - Full Control/All Access (Administrators only)
 - Security full user access (Full user access, PTZ LOCK, no Administrator access)
 - Operational use (Live, Recorded, Alarm, PTZ no LOCK, no Investigation)
 - Custom/Monitoring use (Live, Recorded on per-need basis, PTZ on per-need basis)
- CCTV VMS is not a standard TriMet application. This application requires additional hardware and must be requested through the IT ISSR process.
- Once ISSR is completed CCTV Coordinator will grant rights to CCTV VMS Users, See CCTV SOP SEC101.
- Contact CCTV Coordinator in the Security Division with any questions regarding access or access rights.

Additional CCTV References:

SEC101 SSE-612 – CCTV Camera Installation/Change Request
SEC102 SSE-613 – CCTV Cameras Acceptance (Fixed Facilities)
SEC104 SSE-615 – CCTV Roles and Responsibilities
 HR Policy 207.1 – Information Technology CCTV Use

TRIMET SECURITY	
Fixed: CCTV Roles and Responsibilities (Fixed Facilities)	SEC104 SSE-615
Date: 11-20-14	Page 1 of 2

1.0 Purpose:

This procedure outlines roles and responsibilities for management of TriMet's Closed Circuit Television (CCTV) system.

2.0 Responsibilities:

2.1 Capital Projects

- Procure, plan, schedule, install, and test in-field and in-facility CCTV equipment.
- Coordinate with Security, IT, FEM Communications Department, and Operations to plan camera installation layout and logistics including:
 - Camera placement.
 - Camera coverage.
 - Appropriate camera type for application.
- Research, test, and certify cameras and other end-point devices.
- Coordinate with IT to integrate and test cameras and other end-point devices on-site.
- Document camera maintenance and troubleshooting for FEM Communications Department.
- Provide documentation and information regarding installation, including:
 - Maps and GPS location of cameras.
 - Camera configuration information and settings.

2.2 Safety & Security

- Create and maintain CCTV Video Management System (VMS) usage procedures and policies.
- Receive and process requests for changes to the current camera installation configuration including requests for new camera installations.
- Coordinate with Capital Projects, IT, FEM Communications Department, and Operations to plan camera installation layout and logistics, including:
 - Camera placement.
 - Camera coverage.
 - Appropriate camera type for application.
- Receive, process, and delegate CCTV data access requests.
- Create and maintain camera organization in the CCTV VMS:
 - Camera name and naming scheme.
 - Camera logistical hierarchy (folder structure).
- Create and maintain CCTV VMS settings:
 - Security rights structure.
 - Camera retention standards.
- Review and approve:
 - CCTV user requests.
 - Cameras as acceptable for production.
 - CCTV security change requests
- Put in defect reports to have problems repaired as needed.
- Periodically review the availability of camera views (e.g., image functional or displaying the correct view).

2.3 Information Technology

- Plan, install, maintain, and support network and server technology used in the CCTV architecture:
 - Networks and network hardware.
 - Server and storage hardware.
- Plan, install, maintain and support CCTV VMS software.
- Configure CCTV VMS per policies established by the Security Department.
- Monitor CCTV system components to ensure maximum operability.
- Coordinate with Capital Projects and FEM Communications Department to correct system outages or unacceptable performance.
- Coordinate CCTV system access requests with the Security Department for the installation, maintenance and support of the CCTV client software and customers.
- Coordinate with Capital Projects to integrate, test, and bring cameras into the CCTV VMS software.
- Report on the health of the CCTV VMS and all of its components.

2.4 FEM Communications Department

- Coordinate with Capital Projects on acceptance of maintenance documentation for certified CCTV system equipment, both in-field and in-facility.
- Coordinate with IT to support and maintain in-field and in-facility CCTV system equipment.
- Receive work-orders or other approved communication for repair.
- Perform preventative maintenance inspections.
- Respond to requests for retrieval of data packs from video recording equipment not on the CCTV network.

2.5 Operations

- Monitor the system via viewing stations in the Operations Command Center (OCC).
- Pan Tilt Zoom (PTZ) cameras are to remain trained on their "home" view unless there is a specific business reason to move the camera to view another location. The viewing of cameras positions other than the home view must be limited to legitimate business-related purposes and, if necessary, only with the required permission.
- Report any issues with the system such as no home state to the CCTV Coordinator via e-mail at cctvissues@trimet.org.
- Process requests for images to the Safety and Security Department.
- Security/CCTV Coordinator will notify OCC of any lengthy use of cameras.

Additional CCTV References:

SEC101-SSE-612 – CCTV Camera Installation/Change Request (Fixed Facilities) **SEC102-SSE-613** – CCTV Cameras Acceptance (Fixed Facilities)
SEC103-SSE-614 – CCTV Video Management System User Access (Fixed Facilities) HR Policy 207.1 – Information Technology CCTV Use

Information Technology: CCTV Use

Scope

This policy applies to all TriMet employees and contractors. This policy is administered by and subject to the oversight of the Safety, Security and Environmental Services Department. Violations of this policy are subject to disciplinary action, up to and including termination.

Policy

It is TriMet's policy that CCTV technology is used exclusively to serve security, safety, and operational functions at TriMet and that any incidental personal use is strictly prohibited. CCTV cameras are installed throughout the TriMet system and are used by TriMet employees. Use of this equipment is exclusively for the purpose of monitoring the TriMet rail alignment, bus stops, park and ride facilities, transit centers, stores, money room and other locations, to enhance safety and security, and to identify risks to the system and customers. Adjustments to the position of cameras, aim, direction or focus, and the creation of any recorded images, must be approved by an authorized TriMet manager. The principles outlined in the Basic Information Technology Policy HR-207 apply to use of TriMet's CCTV technology. As with all TriMet equipment, facilities and services, use of CCTV technology by TriMet employees is not personal or private. TriMet may monitor the use of CCTV technology at any time and without advance notice or warning. For purposes of this policy "TriMet Manager" refers to the Deputy General Manager, Executive Director Safety, Security & Environmental, Executive Director Transportation, Director Field Operations, Transportation Managers, Assistant Managers Field Operations, Assistant Managers OCC and Assistant Managers Transportation.

RESPONSIBLE USE

1. When can an employee review, record, download, or transmit a CCTV image?

An employee may only review, record, download or transmit a CCTV image if such action falls within the employee's assigned duties or as specifically directed by an authorized TriMet manager. No employee may provide access to CCTV technology to unauthorized users. An employee may not make adjustments to the focus, brightness or contrast of CCTV cameras unless granted permission by an authorized TriMet manager.

No outside disclosure or transmittal of CCTV is permitted without prior approval of an authorized TriMet manager.

2. What are permissible business uses of CCTV images?

Employees who are authorized to review or transmit CCTV images may use the images only for specified business objectives. Use of CCTV images is primarily confined to the following uses: risk identification and avoidance, claims processing, law enforcement, and general safety and security purposes. The use of CCTV images may be authorized by the Executive Director, Safety, Security and Environmental Services, or designee, in consultation with the Legal Department/Department Executive, for internal training purposes so long as the images do not implicate privacy concerns.

3. Can an employee attempt to view property that is outside a TriMet facility?

Generally, an employee may not aim, direct or focus a CCTV camera (or request this of another employee) onto property adjacent to a TriMet facility. Under special circumstances or in an emergency, an authorized TriMet manager may authorize an employee to view or record adjacent property so long as other legal and ethical considerations (i.e., privacy) are properly observed.

4. May an employee ever view or attempt to view the private space of a person, such as a car or apartment?

No. An employee may not aim, direct or focus CCTV cameras on or into businesses, homes, apartments, vehicles or any other similar private, non-public space, except as necessary to track a fleeing criminal when requested by law enforcement and approved by an authorized TriMet manager.

5. May an employee request to receive historical data from CCTV technology?

Only qualified Transit Police Division, Operations Command Center TriMet managers, Claims Department, or authorized management personnel are allowed to retrieve historical data.

Requests to pull historical data for security related events are to be made by qualified management staff via e-mail to the CCTV Coordinator or Executive Director, Safety, Security and Environmental Services. The CCTV Coordinator will retrieve the data directly. Requests for injury/claims related events are to be made via e-mail to the Risk Management Department. Requests for operations related events are to be made via e-mail to the CCTV Coordinator. Requests to pull historical data must be documented by a completed chain-of-custody request. Current chain-of-custody requests will be used for data pack pull requests for train and bus camera information.

6. Which employees may have CCTV viewing software installed on their PC?

Only employees who have authorization from the Executive Director, Safety, Security and Environmental Services, or designee may have the CCTV viewing software installed on their PC.

7. May Operations Command Center personnel make changes to the home state or zoom level?

Pan Tilt Zoom (PTZ) cameras are to remain trained on their "home" view unless there is a specific business reason to move the camera to view another location. The viewing of cameras positions other than the home view must be limited to legitimate business-related purposes and, if necessary, only with the required permission. Upon completion of the "non-home" viewing, promptly return the camera to its "home" view. If there is a need for a long-term change of view for a specific camera or set of cameras, the request must be approved by the Executive Director, Safety, Security and Environmental Services.

CCTV recorders will record only what is contained in the view that the camera is currently capturing. Cameras must always be aimed, directed or focused on the exact location or event that is to be recorded.

8. May an employee who is involved in an incident request to view the CCTV images of that incident?

Employees involved in an incident may not view the video without permission from an authorized TriMet manager, and may only view the video after completing and submitting an incident report. Viewing the recorded image to assist in writing an incident report may undermine or destroy the value of the incident report as legal evidence.



CCTV Use Policy Receipt (HR 207)

- I acknowledge receiving my own copy of the TriMet CCTV Use Policy (HR 207)
- I am responsible for complying with this policy.

Employee Name (please print)

Emp. #

Employee's Signature

Date