	SAN MARCOS POLICE DEPARTMENT
	Policy 5.3 Computer and Electronic Equipment Usage and Data Security
	Effective Date: March 20, 2017 | **Replaces:** GO 204, 205
	Approved: _____ Chief of Police
	Reference:

I. POLICY

It is the policy of this department to ensure proper use of electronic computing and recording systems by establishing authorized uses and users. This policy states the protocols for storage, security, and retention. It also establishes what uses of such equipment are prohibited and what constitutes inappropriate use of such equipment.

II. PURPOSE

It is the purpose of this policy to define and provide clear direction as to the allowed uses and the prohibited uses of departmental and personal electronic computing and recording equipment, to provide for data security and retention periods, and to establish protocols for proper handling of digital evidence.

III. DEFINITIONS

A. Network Terminals: Desktops, laptops, or any other electronic devices that connect to the department's internal computer network.
B. Mobile Data Terminal (MDT): In-vehicle computers or any other electronic devices that in some manner connect to the Internet, department computer networks, or other service, such as TCIC, that provides officers with data or allows officers to conduct field reporting or communications with other officers or the department.
C. Mobile Phones: Either department owned or personally owned cell phones or smart phones.
D. Body Camera / Digital Media Recorder (DMR): Video/Audio recording equipment that is worn or carried by police personnel.
E. Mobile Video Recorder (MVR): In-vehicle camera systems that are permanently mounted in department vehicles.
F. Digital Media Recordings: Recordings made using a device or system capable of capturing the recording in a digital format.
G. Digital Camera: A single-purpose, handheld camera designed to take digital photographs.

IV. PROCEDURES

The sections below outline the procedures to be used and list the specific prohibitions regarding the use of specific equipment.

A. General Provisions
    1. The following items are considered government records, are subject to public records laws, and shall be preserved accordingly: any electronic document, report, audio or video recording, image, email, voice communication, or any other form of electronic data created while on or off duty that is directly related to official

department operations or investigations, whether created on personal or department-owned equipment.

2. Anything that is created on department-owned equipment, whether or not it is directly related to official department operations or investigations, may be considered a government record, and may be reviewed and shall be preserved as required by state law or department policy. This includes any electronic document, report, audio or video recording, image, email, voice communication, and any other form of electronic data created while on or off duty.
3. The following retention schedule shall be followed for all digital department recordings:
    a. General contacts and misdemeanor offenses – two (2) years
    b. Felony offenses – ten (10) years.
    c. Except as provided by Subsection (d), a recording created with a body worn camera and documenting an incident that involves the use of deadly force by a peace officer or that is otherwise related to an administrative or criminal investigation of an officer may not be deleted, destroyed, or released to the public until all criminal matters have been finally adjudicated and all related administrative investigations have concluded.
    d. The department may release to the public a recording described by Subsection (c) if the department determines that the release furthers a law enforcement purpose.
    e. This section does not affect the authority of the department to withhold under Section 552.108, Government Code, information related to a closed criminal investigation that did not result in a conviction or a grant of deferred adjudication community supervision.
4. Preservation and storage shall be maintained with the video vendor offsite storage solution.
5. All department-owned equipment and its use are subject to routine or specific review and/or investigation by department supervisors as needed to ensure appropriate use.
6. On-duty use of any electronic device, such as a mobile phone or phone camera, for strictly personal purposes not related to departmental operations is generally considered private unless the information would tend to show inappropriate activity. Off-duty use of personal electronic devices is also generally considered private unless the use results in a violation of departmental general orders or state or federal law.
7. Employees that directly access the TCIC/NCIC database shall be trained in the appropriate level of access.
8. If any form of digital evidence exists, formal departmental reports shall include a notation that such evidence exists, including the type of evidence and the storage location.

B. General Prohibitions
    1. Employees shall not release, share, or make copies of any electronic documents, reports, audio or video recordings, images, emails, voice communications, or any

other form of electronic data created while on or off duty that is directly related to official department operations or investigations, whether created on personal or department-owned equipment, outside of the department unless specifically authorized by this order, authorized to continue a criminal investigation or prosecution, or authorized by the chief of police. Criminal statutes may also apply.

2. Employees shall not use department-owned equipment, electronic or otherwise, for personal benefit, use, or to conduct personal business.
3. Employees are allowed to access the internet for personal use during meal and other breaks as long as the sites accessed are appropriate for public viewing.
4. No games shall be played on department equipment.
5. No inappropriate websites shall be visited unless related to an active investigation.
6. Inappropriate use of electronic devices or the release or posting on the internet or various social media sites of another party's private information, or governmental information usually deemed private can lead to internal investigations and subsequent disciplinary action.
7. An officer can be questioned about his/her internet activities by defense counsels in criminal trials, potentially damaging the officer's credibility as a witness.

V. DEPARTMENT NETWORK TERMINALS

A. Security
   1. The department has a number of computers, and other devices, throughout the department that have access to the department network. All employees shall be issued a unique password to allow access to the system.
   2. Employees shall safeguard their password to ensure no other person shall gain access using their password.
   3. Employees shall not leave a computer connected to the network with their password if they are not physically able to prevent access, such as by closing and locking a door, or by visible monitoring of the computer.
   4. Employees are responsible for all access to the network using their password.
   5. The department shall assign appropriate security levels within the network to all access to certain files only as required.

B. Required Access
   1. All employees are required to sign in to the network at least twice each workday (at the beginning and end of their shifts).
   2. Employees must read and respond as needed to all department emails and training assignments.
   3. Employees who discover network terminals in need of repair shall notify the IT helpdesk as soon as possible.

VI. MOBILE DATA TERMINALS

A. Field units subject to calls for service assignments shall be logged onto their mobile data terminal (MDT) and running the computer aided dispatch (CAD) mobile client while on duty.

B. The MDT is a part of the radio system, which uses frequencies licensed by the Federal Communications Commission. Rules concerning proper radio procedures also apply to use of the MDT.
C. Messages
    1. Should be work related.
    2. Should be concise.
    3. Shall not contain derogatory references to other persons or agencies.
    4. Shall not contain any text that a reasonable person would find offensive.
    5. There is NO EXPECTATION of privacy concerning sending or receiving messages via the CAD/MDT system, computer network (including emails), or other department electronic devices.
D. Using the MDT/MDC to decrease radio traffic, field units shall, if tactically feasible and safe to do so,
    1. Check *Enroute*.
    2. Check *At Scene*.
    3. Clear the call.
        a. By going *Available* if not the last on scene, or
        b. Closing with a disposition.
    4. Add appropriate call notes.
       NOTE: Call notes should be updated later if for emergent purposes officers are not able to do so when clearing the call.
    5. Self-initiate their own calls or self-assign to calls where appropriate via the MDT.
        a. Field staff should always consider officer safety and use the radio if necessary.
        b. Field staff shall not self-initiate meal breaks or traffic stops.
    6. Use the MDC for investigative purposes such as checking registration and driver license/warrant information.
    7. Operators should only use the MDC for these purposes from a moving vehicle when the operation can be done with safety. When such activity would be considered unsafe, operators should utilize the police radio for this activity.
E. Employees who discover their MDT in need of repair shall notify their supervisor and the IT helpdesk as soon as possible. They shall also ask their supervisor to secure them a spare MDT from one of the designated spare laptop storage locations.

VII. MOBILE VIDEO RECORDING SYSTEMS

A. The use of a Mobile Video Recording (MVR) system provides persuasive documentary evidence and helps defend against civil litigation and allegations of officer misconduct. Such evidence is often used in court cases, and can help in determining the guilt or innocence of accused people.
B. Officers assigned the use of these devices shall adhere to the operational objectives and protocols outlined herein so as to maximize the effectiveness and utility of the MVR and the integrity of evidence and related video documentation.
C. General Procedures

1. It shall be the responsibility of this department to ensure that the audio-video recording equipment is properly installed according to the manufacturer's recommendations.
2. MVR equipment shall automatically activate when emergency equipment (lights) or a wireless transmitter is operating.
3. The system may also be activated manually from the control panel affixed to the interior of the vehicle.
4. Placement and operation of system components within the vehicle shall be based on officer safety requirements.
5. All officers shall successfully complete this department's approved course of instruction prior to being deployed with MVR systems in operational settings.
6. Inspection and general maintenance of MVR equipment installed in departmental vehicles shall be the responsibility of the officer assigned to the vehicle.
7. Prior to beginning each shift, the assigned officer shall perform an inspection to ensure that the MVR is performing in accordance with the manufacturer's recommendations covering the following matters:
    a. Remote activation of system via transmitter
    b. Windshield and camera lens free of debris
    c. Camera facing intended direction
    d. Recording mechanism capturing both audio and video information, that is, the system plays back both audio and video tracks.
8. Malfunctions, damage, or theft of in-car camera equipment shall be reported to the immediate supervisor prior to placing the unit into service.
9. Mandatory Use
    a. All official contacts whether on a call or officer initiated.
    b. Traffic stops (to include, but not limited to, traffic violations stranded motorist assistance, and all crime-interdiction stops).
    c. Priority responses.
    d. Vehicle pursuits.
    e. Prisoner transports.
10. When the MVR is activated, officers shall ensure that the audio portion is also activated so that all events are properly documented. Officers are encouraged to narrate events using the audio recording, which shall provide the best documentation for pretrial and courtroom.
11. Officers shall not erase, alter, reuse, modify, or tamper with MVR recordings.
12. When the MVR is activated to document an event, it shall not be deactivated until one of the following has occurred:
    a. The event has been concluded.
    b. The incident or event is of such duration that the MVR may be deactivated to conserve recording times.
    c. The employee decides that deactivation will not result in the loss of critical documentary information.
    d. The intention to stop the recording has been noted by the employee either verbally or in a written notation.

13. Supervisor Responsibilities
    a. When an incident arises that requires the immediate retrieval of the recorded media (e.g., at serious crime scenes, departmental shootings, or departmental accidents), a supervisor shall ensure recordings are uploaded.
    b. Supervisors who are informed or otherwise become aware of malfunctioning equipment shall issue replacement equipment and ensure malfunctioning equipment is sent for repairs.
    c. At least four times per calendar quarter, supervisors are responsible for conducting a review of random samplings of at least one quarter of their subordinates' evidentiary and non-evidentiary video recordings.
        i. When determining the number of subordinates to be reviewed, fractions are to be rounded up to the next whole number.
        ii. The supervisor shall use the appropriate form to document the review and forward it to the respective commander.
        iii. Audits are to be due in January, April, July and October.
    d. In the following circumstances, the on-duty supervisor shall conduct a video review before approving any offense and/or use of force reports. In these cases, it is not necessary to review all videos associated with the incident or the entirety of any one video if a reasonable conclusion can be drawn by reviewing less video footage. The supervisor shall note their video review in the appropriate comments field in Blue Team during the approval process. In instances which do not involve the use of Blue Team, the supervisor shall notify their commander of this review by email after it is completed.
        i. All arrests resulting in charges for Resisting Arrest, Detention, or Transportation or Assault on a Peace Officer.
        ii. All uses of force involving the actual use of an intermediate weapon including the Taser.
    e. A supervisor shall take appropriate action to address any policy, training, or performance issues that arise as a result of the review process. Any issues involving officer misconduct or violations of departmental policies or procedures shall be handled as proscribed in department policy.
    f. If a citizen complaint is lodged against an officer who was using recording equipment, the supervisor shall obtain the recording of the alleged incident. The complaint shall be handled according to departmental procedure, and a copy of the recording will become a part of that investigative record.
    g. Supervisors shall conduct quarterly inspections of issued equipment to evaluate its suitability for its intended use. If defects are discovered, the unit shall be removed from service and the appropriate Commander notified through the chain of command.
    h. Those reviewing recordings should be aware that the video camera is two dimensional and may not capture everything as seen by the wearer. Due to the position of the camera, the view may be blocked by the wearer's arms, hands, or other objects as the wearer moves or engages with a member(s) of the public.

14. Uploading MVR Recordings
    Recordings are to be uploaded to storage device/cloud
    a. By the end of shift any time a recording will be considered as evidence and retained as such.
    b. At the end of the employee's shift if driving any vehicle other than their assigned vehicle.
    c. By the end of the employee's work week at all times.

VIII. MOBILE TELEPHONES

A. Department Issued Cell Phones
    1. Cell phones are issued by the department to increase the level of communication between field employees and the department as well as citizens.
    2. Cell phones should be turned on and immediately accessible while on duty.
    3. Cell phones are to be used for appropriate departmental activities only.
    4. Employees are allowed to use department cell phones for emergency and short personal calls during breaks.
    5. The department may inspect cell phone usage records for inappropriate activity.

B. Personally Owned Cell Phones
    The department allows employees to carry personally owned cell phones when their use does not negatively impact department operations.

IX. CELL PHONE CAMERAS

A. Departmental Cell Phones
    1. All activities recorded on cell phone cameras shall be transferred immediately to departmental records systems as soon as the incident can be concluded and no later than the end of shift.
    2. Cell phone cameras, both still and video, using the QueTel App is the preferred method to record department activities. QueTel is the preferred camera upload for digital evidence.
    3. Activities may include victim, witness, or suspect information, crime scenes, field and eyewitness identifications, witness statements, etc.

B. Personal Cell Phones
    1. Personal cell phone features (or apps), both still and video, may be used to record department activities only when another more suitable digital camera or recording device is unavailable.
    2. If any department activity is recorded using a personal cell phone, a supervisor shall be notified immediately.
    3. All activities recorded on cell-phone cameras shall be transferred immediately to departmental records systems as soon as the incident can be concluded and no later than the end of shift.
    4. After transfer to departmental media, all parts of the activity recorded shall be permanently deleted from the personally owned cell phone prior to end of shift. Supervisors may require proof of deletion.

X. DIGITAL CAMERAS

A. Department Issued Cameras
    1. Personnel assigned to crime scene investigations have available other department camera systems for recording crime scenes and incidents.
    2. Officers are assigned cell phones to record images and data beneficial to an investigation when crime scene personnel do not respond.
    3. Department-issued cameras shall not be used for any personal use.
    4. All images or data recorded shall be transferred to appropriate departmental media or storage before the end of shift. The QueTel App is the preferred method to record department activities. QueTell is the preferred camera upload for digital evidence.

B. Personally Owned Cameras
    1. No employee shall carry a personally owned camera on duty unless authorized in writing by the chief of police.
    2. If a personally owned camera has been authorized in writing by the chief of police, the employee shall report any use of the camera during a police incident to their supervisor immediately and shall transfer the data to department media before the end of shift.
    3. After transfer to departmental media, all parts of the activity recorded shall be permanently deleted from the personally owned camera prior to end of shift. Supervisors may require proof of deletion.

XI. DIGITAL MEDIA RECORDERS

These procedures apply to body worn cameras and other portable audio/video recorders primarily for uniformed employees. Refer to specific investigative policies for usage by detectives during follow-up investigations and/or undercover operations. These procedures do not apply to mounted in-vehicle audio/video systems, which are covered elsewhere in this order.

A. Department Issued Digital Media Recorders (DMR)
    1. All digital multimedia evidence that is captured during the scope of an employee's duties is the property of the department and shall not be converted or copied for personal use. Accessing, copying, editing, erasing, or releasing recordings or depictions of recordings without proper approval is prohibited and subject to disciplinary action.
    2. Employees issued a DMR shall use the device as required in the following sections with the exception of detectives, who shall comply with directives for follow-up investigations and undercover operations.

B. When Usage is Required

    If the DMR is activated for any of the reasons listed below, the recording shall continue until the incident is complete or the employee has left the scene. An employee who wishes to engage in a discussion with another department employee relating to the contact may mute the microphone only when away from the suspect or subject. The microphone must be re-activated as soon as the suspect or subject is contacted again so that all contact between the employee and suspect or subject is recorded.
    1. During any citizen contact outside the employee's vehicle.

2. During any interview with a victim, witness, or suspect.
3. During any field or eyewitness identification.
4. During any enforcement contact when the employee is outside his/her vehicle.
5. During building searches and alarm responses.
6. During any uniformed "extra duty" work in which the above conditions occur.

C. Prohibitions
   1. Employees shall not intentionally create digital recordings of other employees in areas where a reasonable expectation of privacy exists.
   2. Employees should consider turning off the DMR when in areas where a reasonable expectation of their own privacy exists.
   3. Employees shall not intentionally create digital recordings of citizens' activities in areas where a reasonable expectation of privacy exists, unless the recording is made while the officer is legally in the area for one of the situations listed in section B above. Employees should be aware that under certain circumstances, e.g. victims or suspects in various stages of undress, the employee may consider stopping the recording and shall explain the stopped recording in the report.
   4. Employees shall not knowingly record undercover officers or informants.
   5. Employees shall not use a departmental device to record any personal activities.
   6. Officers shall not allow any non-sworn personnel to view the DMR or any other recorded data without the permission of the officer's supervisor.
   7. Uploading of any DMR data to any social media site is prohibited.
   8. Employees may use DMRs only in-patient care areas of hospitals or emergency rooms when the recording is for official business.
   9. To the extent possible, employees shall attempt to prevent the recording of non-involved individuals.

D. Employee Responsibilities
   1. Employees issued a department-owned DMR shall attend training, and they shall demonstrate proficiency with the recording and transfer of recorded data.
   2. Employees shall inspect the device at the beginning of each shift to ensure proper operation, including sufficient battery life and recording medium.
   3. Any device found deficient at any time shall be reported to the employee's supervisor who shall issue a replacement if one is available.
   4. Uploading DMR recordings.
      Recordings are to be labeled and uploaded to the storage device/cloud:
      a. Considering the size of videos, labeling process and download time, the best practice is an upload of videos daily, and is required either at the end of shift, or;
      b. Prior to the beginning of the next shift, and;
      c. By the end of the employee's work week at all times.

E. Personally Owned Digital Media Recorders (DMR)
   Are not allowed or permitted on-duty.

F. Supervisor's Responsibilities

1. When an incident arises that requires the immediate retrieval of the recorded media (e.g., at serious crime scenes, departmental shootings, or departmental accidents), a supervisor shall ensure recordings are uploaded.
2. Supervisors who are informed or otherwise become aware of malfunctioning equipment shall issue replacement equipment and ensure malfunctioning equipment is sent for repairs.
3. At least four times per calendar quarter, supervisors are responsible for conducting a review of random samplings of at least one quarter of their subordinates' evidentiary and non-evidentiary video recordings.
    a. When determining the number of subordinates to be reviewed, fractions are to be rounded up to the next whole number.
    b. The supervisor shall use the appropriate form to document the review and forward it to the respective commander.
    c. Audits are to be due in January, April, July and October.
4. In the following circumstances, the on-duty supervisor shall conduct a video review before approving any offense and/or use of force reports. In these cases, it is not necessary to review all videos associated with the incident or the entirety of any one video if a reasonable conclusion can be drawn by reviewing less video footage. The supervisor shall note their video review in the appropriate comments field in Blue Team during the approval process. In instances which do not involve the use of Blue Team, the supervisor shall notify their commander of this review by email after it is completed.
    a. All arrests resulting in charges for Resisting Arrest, Detention, or Transportation or Assault on a Peace Officer.
    b. All uses of force involving the actual use of an intermediate weapon including the Taser.
5. Supervisor shall take appropriate action to address any policy, training, or performance issues that arise as a result of the review process. Any issues involving employee misconduct or violations of departmental policies or procedures shall be handled as proscribed in department policy.
6. If a citizen complaint is lodged against an employee who was using recording equipment, the supervisor shall obtain the recording of the alleged incident. The complaint shall be handled according to departmental procedure, and a copy of the recording shall become a part of that investigative record.
7. Supervisors shall conduct quarterly inspections of issued equipment to evaluate its suitability for its intended use. If defects are discovered, the unit shall be removed from service and the appropriate Commander notified through the chain of command.
8. Those reviewing recordings should be aware that the video camera is two dimensional and may not capture everything as seen by the wearer. Due to the position of the camera, the view may be blocked by the wearer's arms, hands, or other objects as the wearer moves or engages with a member(s) of the public.

G. Release of information Related to Body Worn Camera Recordings

1. Refer to Occupations Code, Sections 1701.661; 1701.662; 1701. 663 for further information.