Brief reason for the revision:

Criminal Justice Information Systems (CJIS) security policy restricts the user's ability to send Criminal Justice Information over a non-compliant CJIS platform.

1004 Department Owned Cell Phones

1004.2 CELL PHONE GUIDELINES

Employees shall adhere to the following guidelines when using any Department issued cell phone:

- (a) Employees issued a Department cell phone will ensure the device is operational and in their possession at all times while on duty or working law enforcement related secondary employment. The Department's cell phone shall remain within the United States.
 - On-duty non-exempt employees shall respond to any Departmental phone calls, texts, and voicemails which that require a response, as soon as practicable.
 - 2. Off-Duty non-exempt employees will respond to Departmental phone calls, texts, and voicemails once they return to work.
 - 3. Exempt employees shall respond to any Departmental phone calls, texts, and voicemails which that require a response, as soon as practicable.
 - 4. Cell phones are not the primary source for urgent communications as they can be unreliable during large events where technology usage is high. Messages requiring an immediate response or that are urgent in nature (e.g., SWAT call out) should be sent using a designated City of Austin messaging system (e.g., Wireless Office, SPOK, CAD).
- (b) Employee use of the cell phone shall be professional, polite, civil, and orderly, treating all persons with fairness, dignity, and respect.
- (c) Employees shall select ring tones and audible alerts from factory-provided options on the cell phone and shall not download or install other ringtones or audible alerts.
- (d) When making phone calls or texts for Department business, employees should identify themselves as members of the Austin Police Department and clearly state the purpose of the call unless doing so would compromise the integrity of a criminal investigation.
- (e) In general, employees should not give out Department issued cell phone numbers unless:
 - Immediate contact between a police employee and a victim, witness, or etheranother person may be critical.
 - 2. The employee to whom the cell phone is assigned has granted authorization.; or
 - 3. A supervisor authorized the release of the number. Release of the number was authorized by a supervisor.
- (f) Telephones shall be placed in a-vibrateion or silent mode while attending court and They may be placed in a-vibrateion or silent mode while attending training, meetings, and any other time needed to prevent interruption or annoyance.
- (g) All cellular telephone calls, text messages, emails, and other communications may be subject to discovery in criminal or civil matters, may be subject to release to a member of the public in response to a public information request, or may be used in internal

investigations. All communications, unless an emergency, should be related to Department business.

- Employees should consider these communications a public record and should have no expectation of privacy.
 - (a) Text messages of evidentiary value shall be screenshot and processed according to per General Order 618.5 (Digital Evidence Collection and Storage).
 - (b) Voicemails of evidentiary value shall be played with the speakerphone activated and recorded with the BWC recording system.
 - (c) Photos and videos of evidentiary value shall be processed according to General Order 618.5 (Digital Evidence Collection and Storage).
- 2. Employees must not delete any items of evidentiary value from their cell phone.
- (h) For safety and accountability, employees shall ensure that location services (GPS) are enabled while on duty, including any LERE secondary employment.
- (i) The Department reserves the right to access any information on Department-issued cell phones. Supervisors will-refer to General Order 902.6.1(c) for guidance.
- (j) Upon separation from Department employment, all Department-issued cell phones shall be returned to Police Equipment or the employee's supervisor.
- (k) Criminal Justice Information (CJI) can only be transmitted to internal APD users via the Outlook App on Department Issued Cell Phones. CJI includes data derived from the Department of Public Safety or the Federal Bureau of Investigation through systems such as TLETS and TCIC/NCIC. Sensitive information includes, but is not limited to, CCH, CHRI, Social Security numbers, and credit card numbers. This information shall not be sent by text message.