EFFECTIVE: 6 April 2009

REVISED: 1 January 2010
20 June 2011
18 December 2013

SUBJECT: Electronic Communications – Acceptable Use

ISSUED BY: Fernando Solorzano

I. PURPOSE

The purpose of this policy is to establish procedural guidelines for the use electronic communications systems, including activity involving the Internet and Police Data Network (PDN), individual workstations and mobile devices, and access to data stored in local, state, and federal computer systems. Electronic mail and faxes, which are transmitted over the Internet, PDN, wired or wireless telephone or data systems are subject to all provisions of this policy.

II. AUTHORIZED PERSONS

Access to computers, networks, and electronic communications on behalf of the Department is limited to employees, volunteers, authorized vendors, and contractors.

kept for at least 30 days unless compromised. Passwords must not be written down and may never be shared.

Employees with remote access tokens may not write down their PIN code and must advise the Information Management Bureau (IMB) immediately whenever a token is lost or stolen.

VI. STANDARDS AND OPERATIONS

The IMB is responsible for selecting and purchasing the standard desktop software suite for all departmental computers and for the administration of the software on all computers connected to the PDN.

All employees shall use the department's selected desktop software unless critical functionality is not available through the application. Specialized software needs will be assessed on an individual basis and, not withstanding technical conflicts, installed upon the approval from IMB and the Division Commander.

(a) INSrJ ELMrriINSrJ ELM

(d) PROHIBITED USE

At no time during a response to a call for service will any employee of this department on or off-duty make any posting or send any message or notification to any social networking site, listserve or texting resource/outlet that comments in any way upon that departmental response unless directed to do so by a commanding officer and as part of a tactical response to that call for service.

(e) **EMAIL**

(1) USE

All employees shall check their campus email daily, s-4 (l) 0 Td ( )Tw -vte(t)-S1

c. The forwarding of chain letters, junk mail, and executables is strictly forbidden
d. Do not send mass mailings
e. All messages distributed via the campus email system, even personal emails, are property of the Department and the University.

(f) TEXT MESSAGING

(1) USE

The purpose of this order is also to establish guidelines for the proper use and application of text messaging by employees of this department. This order refers to all department-issued electronic communication devices and includes all mobile phones, PDA's, pagers, and any other such wireless two-way communication devices.

Text messaging is a tool available to some employees as a means to enhance efficiency in the performance of job duties and is to be used in accordance with generally accepted business practices and current law. Messages transmitted on a text messaging system must only be those that involve official business activities or contain information essential to employees for the accomplishment of business-related tasks and/or communication directly related to the business, administration, or practices of the department.

(2) PRIVACY

All text messages transmitted on equipment issued by the Department are considered Department records and, therefore, are property of the Department. The Department reserves the right to access, audit, monitor, and disclose, for whatever reason, without notice to employees, all messages, including text transmitted on Department equipment. Text messages are not appropriate for personal communications. Three is no expectation of privacy in the use of Department-issued equipment.

(3) PROHIBITED USE

Sending or forwarding derogatory, defamatory, obscene, disrespectful, offensive, racist, sexually suggestive, and harassing or any other inappropriate messages via text message is prohibited and will not be tolerated.

(3) PROHIBITED USE
Level 1 Confidential and CLETS-provided information may not be stored on any device except for department-owned encrypted devices specifically issued for that purpose.

(4) PERSONAL USE
Incidental personal use of both personally-owned and department-owned devices is permitted, subject to the operational and privacy restrictions described in this section.

APPROVED