OFFICE OF THE CHIEF OF POLICE

NOTICE

September 24, 2019

14.5

TO: All Department Personnel

FROM: Chief of Police

SUBJECT: OPERATOR SECURITY STATEMENT – RENAMED AND REVISED

The Operator Security Statement, Form 01.58.00, has been revised and renamed as the Los Angeles Police Department Information Security Agreement, Form 01.58.00.

The revised form was drafted to add new technologies, Department mobile devices, and the use of e-mail which contributes to 90 percent of data breaches. Additionally, this form serves to remind Department personnel that there is no expectation of privacy in the use of Department devices.

This form is typically signed by employees when they are newly hired to the Department. The form will be redistributed through the Department's Learning Management System (LMS) every two years.

Any questions regarding this Notice may be directed to the Forms Unit, Risk Management and Policies Division, at (213) 486-0405.

MICHEL R. MOORE
Chief of Police

DISTRIBUTION "D"

Attachment

LOS ANGELES POLICE DEPARTMENT
INFORMATION SECURITY AGREEMENT

The information below defines the Los Angeles Police Department Information Security Agreement provision:

1. The Los Angeles Police Department policy classifies the following as confidential: official files, documents, records, reports and information held by the Department. Authorized regular and contracted employees are prohibited from disclosing any information from these sources except in the scope of their employment [Los Angeles Police Department (LAPD) Manual Section 3/405].

2. The Los Angeles Police Department automated stored information systems shall not be used for the dissemination of Department of Motor Vehicles (DMV) and Criminal Offender Record Information (CORI) to any other agency or person for purposes of employment, licensing, or certification. Under no circumstances shall DMV and/or CORI be released to the news media or their representatives.

3. All access to California Law Enforcement Telecommunications Systems (CLETS) related information is based on the "need to know" and the "right to know." Misuse of such information may adversely affect an individual's civil rights and violates the law and/or CLETS policy.

4. I will treat all unpublished LAPD electronic data and information as confidential and will not disclose or disseminate it without prior authorization.

5. I have received access authorization (Serial No. and password), and I shall consider this information confidential and to be used only by me. I shall not operate a computer without first inputting this information into the computer. I am responsible for all inquiries originated from the computer while I am signed on until I receive positive acknowledgement of my sign-off (LAPD Manual Section 3/788.20).

6. I will not solicit, possess, or seek the use of any password other than that which has been officially issued to me by the LAPD.

7. It is my responsibility to inform my supervisor if I am requested to make any inquiry or other transaction by any person who is not authorized to receive the data.

8. All transactions performed through automated information systems administered by the Information Technology Division of the LAPD, or through other City-owned or City-controlled automated information systems, may be logged, and that use of these systems is subject to continuous monitoring.

9. All information (including all e-mails and personal entries) which I input, process, transmit, store, save, download, or receive on LAPD computers, mobile devices, or peripherals remains, at all times, subject to retrieval, reconstruction, review, and investigation by the LAPD, and does not have or give rise to any expectation of privacy on my part.

10. I will use LAPD computers, mobile devices, and peripherals for LAPD business purposes only, regardless of the place or mode of access, including access to the Internet/Intranet.

11. All e-mails shall be used for LAPD business purposes. The LAPD reserves the absolute right to review, audit, and disclose any e-mail message sent over the system or placed into its storage. All e-mail messages composed, sent, and received are and remain the property of the LAPD. The LAPD can monitor e-mails for any reason and without limitation.

12. California Penal Code Section 502, prescribes the penalties relating to computer crimes. California Penal Code Sections 11105 and 13300 identify who has access to criminal history information and under what circumstances it may be released. California Penal Code Sections 11141-11143 and 13302-13304 prescribe penalties for misuse of criminal history information. California Government Code Section 6200 prescribes the felony penalties for misuse of public records and CLETS information. California Vehicle Code Section 1808.45 prescribes the penalties relating to misuse of Department of Motor Vehicles record information.

I, THE UNDERSIGNED, ACKNOWLEDGE RECEIPT OF THE LOS ANGELES POLICE DEPARTMENT INFORMATION SECURITY AGREEMENT AND AGREE TO COMPLY WITH ITS PROVISIONS AS DEFINED ABOVE.

I FULLY UNDERSTAND THAT ANY VIOLATION OF THE LOS ANGELES POLICE DEPARTMENT INFORMATION SECURITY AGREEMENT MAY RESULT IN DISCIPLINE, UP TO AND INCLUDING DISCHARGE, AS WELL AS POSSIBLE CIVIL AND CRIMINAL LIABILITY.

MY SIGNATURE BELOW INDICATES THAT I HAVE READ, UNDERSTOOD AND ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT. I FURTHER ACKNOWLEDGE I HAVE RECEIVED A COPY OF THIS FORM.

Print Name: _____

Serial No./Employee No.: _____

Department/Division: _____

Signature: _____ Date: _____

FOR OUTSIDE CONTRACTOR USE ONLY:

Contractor Firm Name: _____

Contractor Address: _____

Contractor Phone No.: _____

Supervisor Signature: _____ Date: _____