INFORMATION TECHNOLOGY BUREAU

NOTICE July 31, 2014
17.1

TO: All Department Personnel

FROM: Commanding Officer, Information Technology Bureau

SUBJECT: GUIDELINES FOR MAINTAINING USER CREDENTIAL CONFIDENTIALITY

This Notice is intended to remind all Los Angeles Police Department (LAPD) employees of the importance of properly securing user IDs and passwords (user credentials) to prevent unauthorized persons from accessing systems containing law-enforcement sensitive information administered by the LAPD, its partners and affiliates. This includes user credentials associated with all Department-issued computers (desktop and portable), smartphones and storage devices (connected via USB or by Ethernet), as well as mainframe or server-based applications, databases, files and smartphone apps that are accessed on these devices.

All users who have been authorized to use the Department's computers have signed an Operator Security Statement that indicates acceptance by the signatory of the duties and responsibilities described therein. Ignorance or purposeful non-compliance with these requirements can subject the violator to significant penalties.

The following guidelines shall be followed by all employees in regard to the management of user credentials. These guidelines are effective immediately upon the publication of this Notice.

#	CREDENTIAL CONFIDENTIALITY GUIDELINE	EXAMPLE(S) TO AVOID
1	All passwords used by employees on all systems and devices provided by the LAPD shall contain a combination of upper and lower case letters, with numbers and symbols (i.e., "strong" passwords.)	Short and simple passwords.
2	An employee may not share any user credentials used for accessing any computer system or device, used for conducting Department or City business, with any other person for any reason, without the approval of the Commanding Officer, Information Technology Bureau or designee.	Sharing credentials with a co-worker.

#	CREDENTIAL CONFIDENTIALITY GUIDELINE	EXAMPLE(S) TO AVOID
3	An employee's passwords must never be recorded in any location that permits any other person to view them, or to allow an unauthorized person to gain access to them.	Putting a note with passwords upon one's computer monitor. Posting a password in a publicly viewable location.
4	Providing access to a Department computer, the Department network or other computer systems that are used for Department business, to persons who have not passed the Department's fingerprint-based background check.	Providing your credentials to an unauthorized person so that they can login using your credentials.
5	Accessing CLETS resources/CJIS protected data remotely without using a second factor of authentication from a mobile device without the approval of your Commanding Officer and the approval of Commanding Officer, Information Technology Bureau. The definition of mobile device herein does not include portable computers mounted and used solely inside Department vehicles.	Accessing CLETS from a smartphone or tablet without using a second factor of authentication, such as a token, one-time password or any similar method of authentication.

If you have any questions regarding this Notice, please contact Senior Systems Analyst Sanjoy Datta, at (213) 486-0270.

APPROVED:

MAGGIE GOODRICH, Chief Information Officer
Commanding Officer
Information Technology Bureau

STEPHEN R. JACOBS, Deputy Chief
Chief of Staff
Office of the Chief of Police

Distribution "D"