

Ensuring Confidentiality and Integrity of County Information Technology Systems

The County of Los Angeles (County) heavily depends on information technology (IT) to run its daily operations and deliver vital services to its residents. It is critical that the County diligently manages its IT systems to ensure confidentiality is protected, the integrity of data is maintained and security risks are avoided.

Recently, in compliance with Countywide IT Policy 6.108 (Auditing and Compliance Policy), the Auditor Controller conducted a thorough Information Technology and Security Policy review for the Probation Department and Department of Public Health. Those audits revealed serious flaws. Both departments did not deactivate hundreds of terminated employees' accounts, thereby allowing former employees to retain access to sensitive information. Both departments also did not maintain accurate IT equipment inventories, resulting in misplaced desktops, laptops and other IT devices that may contain sensitive information. Both departments submitted corrective actions.

To date, six departments, out of a total thirty three departments, have been audited for compliance.

The County must make IT security a top priority.

- MORE -

MOTION

SOLIS _____

RIDLEY-THOMAS _____

KUEHL _____

KNABE _____

ANTONOVICH _____

**MOTION BY SUPERVISOR MARK RIDLEY-THOMAS
JULY 14, 2015
PAGE 2**

I THEREFORE MOVE THAT THE BOARD OF SUPERVISORS:

- 1) Direct the Auditor Controller, in coordination with the Interim Chief Executive Officer, to report back in 60 days on the feasibility of conducting Information Technology and Security Policy Reviews for every County department, including the Chief Executive Office and Executive Office, on an annual basis; and
- 2) Direct the Interim Chief Executive Officer to require any department or office with Information Technology security vulnerabilities, as identified by the Auditor Controller, to submit detailed reports to the Board of Supervisors, Auditor Controller and the County Chief Information Security Officer every 90 days on the progress being made to correct each security vulnerability and the steps being taken to prevent further future problems until each identified vulnerability is fully corrected.

####

(YV/MA)