File #: A 21-456, **Version:** 1

Approve and adopt the Monterey County Security Policy as updated/amended.
RECOMMENDATION:
It is recommended that the Board of Supervisors:
Approve and adopt the Monterey County Security Policy as updated/amended. Updates are necessary to cope with an increasingly complex technological environment and to meet constantly evolving security challenges.

SUMMARY/DISCUSSION:
On May 13, 2014, the Monterey County Board of Supervisors adopted the County's current version of the Information Technology Department's Security Policy. Recently changes to the policy have been made necessary due to changes in technology, as well as a change in the security framework the County is using to measure the gaps and capabilities of its cybersecurity programs.

The changes are as follows:
1.1 STANDARDS In addition to County Information Security Standards documents established and maintained by the Chief Security and Privacy Officer, the County shall adopt the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (also known as the NIST Cybersecurity Framework). This Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today. This Framework is the basis for the County's required annual Nationwide Cybersecurity Review self-assessment, designed to measure the gaps and capabilities of state, local, tribal and territorial governments' cybersecurity programs.

Reason for change: Local governments across the country have shifted to using the NIST Framework to provide standards, guidelines, and best practices. The County of Monterey is regularly reviewed through the annual Nationwide Cybersecurity Review self-assessment based upon this standard, and this assessment is used to qualify for the Homeland Security Grant Program that funds certain County programs. Additionally, language regarding this framework has been provided to County Counsel's committee on updates to the standard agreements, to provide security language built-in to our contract language for doing business with IT vendors. This framework replaces the ISO/IEC 27002 standard currently written in the Security Policy.

1.9.8.1 In the event of a security issue with a "personally-owned" device, the owner of the device is required to remediate all issues before utilizing the device to access any county resources.

Reason for change: This added language affirms the employee's responsibility for assuring their personally-owned devices are secure before accessing County data.

1.10.3. For County applications and services that are available for login on the Internet, the application or service shall be configured so that an outside attacker with a stolen password cannot login to the service.

Reason for change: The County is constantly battling credential theft and is rolling out advanced authentication and "single sign on" technologies to mitigate this threat. This language requires that department

applications and services adopt this available technology or other appropriate technologies to mitigate this threat to their Internet-available applications.

1.10.9,1.10.10 - Language updates

Reason for change: Removal of older language, reflecting the County's adoption of the newer NIST password policies that were adopted by the department heads in October of 2017.

1.9.1.4, 1.9.5, 1.9.14, 1.13.3.1, 1.14.2.1, 1.14.3.1.10, 1.14.3.1.11, 1.17.2.1.5, 1.17.4.1.3, 1.18.3.3.2.3 - Terminology updates

Reason for change: Various terminology changes reflecting current technology and state of threats against the County. No impact on intent of policy.

A table of contents has been added.

OTHER AGENCY INVOLVEMENT:
The Information Security Officers within each department were provided opportunity to provide input on these changes. County Counsel has also reviewed these changes.

FINANCING:
There will be no direct financial impact caused by these policy wording changes.

BOARD OF SUPERVISORS STRATEGIC INITIATIVES:
Cyber Security and the protection of the information that the County is responsible for supports all the Board of Supervisors Strategic Initiatives.

X Economic Development
X Administration
X Health & Human Services
X Infrastructure
X Public Safety

Prepared by: Daniel Kern, Chief Security Officer, x1449

Approved by:

_____ Date: _____
Eric A. Chatham, Director of Information Technology, 759-6920

Attachments:
Security Policy - 2021 Changes