Attachment 2

IT Security Program Implementation Plan – ITAM-0601

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	IT SECURITY PROGRAM IMPLEMENTATION PLAN	ITEM NUMBER:	ITAM-0601
OWNER:	DEPARTMENT OF GENERAL SERVICES	ADOPTION DATE:	MM/DD/20YY
APPROVER(S):	COUNTY BOARD OF SUPERVISORS	REVIEW DATE:	MM/DD/20YY
VERSION:	1.0	PAGE:	PAGE **1** OF **3**

I. Purpose

The purpose of this IT Security Program Implementation Plan is to recognize and declare that compliance to the Technical IT Security Policies is a goal that will take time to fully implement, and to set the expectation that full compliance will be met as soon as practical but no later than three years.

II. Audience

The primary audience for the Technical IT Security Policies is Information Technology Professionals (County executives, managers, employees, contractors, vendors and third parties) whose responsibilities include deploying, managing, administering and operating all County Technology Assets (hardware, software, data systems, Cloud environments, SAAS, technology contracts, the Internet of Things (IOT), etc.).

III. Scope

The Technical IT Security Policies apply to any Information System that electronically generates, receives, stores, processes or transmits County-owned data, whether the system is hosted on the County network or by a third-party provider. The Technical IT Security Policies are directed to all County technology personnel supporting the deployment of any technology assets in the County including 'on premise', remotely, in the Cloud, Hosted, or otherwise and includes hardware, software, application and environmental (hardware) services, application and database development and support, the Internet of Things (IOT), and all other technical aspects of County business.

Additionally, these provisions apply to anyone doing business as the County and/or in support of the County that is provisioned access to County technology assets and/or systems. This includes employees, contractors, consultants, temporaries, and other workers at the County, including all personnel affiliated with third parties, collectively referred to hereafter as "agents".

IV. Definitions

See ITAM-0602, Glossary of Definitions

V. Policy

The Technical IT Security Policies are intended to provide an avenue of compliance to security 'best practices' according to the National Institute of Standards and Technology (NIST) Security Guidelines. They are adopted by the County of Santa Barbara as base standards to protect all County technology assets including data and information as well the ability to provide, with minimum interruptions, the technology needed to meet the business needs of our stakeholders in process availability.

Although the expectation is to meet all these policies and procedural requirements as soon as possible (to minimize the on-going risks to individual departments as well the County as a whole), it is acknowledged that it will not be easy to immediately meet these baseline security requirements. Remediation to bring security up to this baseline level must be completed as soon as possible and no later than three years after the initial adoption date of the County IT Security Policy package.

Departments are required to document and track all control weaknesses. Central IT and the County CISO will provide tools to track County progress in meeting these minimum security requirements. For all technology that currently cannot meet the security control requirements designated within IT Security Program and Associated Policies, departments are required to develop remediation plans to address identified issues within the 3-year timeframe and to use the County GRC system with ServiceNow (or other provided tools) to continually update and track progress in meeting these policies.

The CISO is responsible for reviewing progress to identify areas of high risk needing immediate mitigation and working with departments to implement timely mitigation actions. Security remediations requiring resources outside of department budgeted funding will be reported to the EITC and the Budget Director.

Any and all deviation requests from meeting these policies will require an appropriate 'risk/threat' analysis and a final acceptance or approval from the County CISO for further continuance of that area of security addressed by the request.

As additional resources, Central IT and the CISO are available to help Departments meet these policy requirements.

VI. Exceptions

See ITAM-0600, IT Security Program

VII. Non-Compliance

See ITAM-0600, IT Security Program

VIII. References and Sources

1. Applicable Rules, Laws, and Regulations:
2. Related Policies:
3. Referenced Documents:

4. Revision History:

VERSION	CHANGE	AUTHOR	DATE OF CHANGE
1.0	Initial Release	CISO/Policy Committee	08/25/2021