COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY STANDARD REQUEST

SUBJECT:	PASSWORD MANAGEMENT & DIGITAL VAULT	ADOPTION DATE:	MM/DD/20YY
REQUESTER:	EXECUTIVE INFORMATION TECHNOLOGY COUNCIL		
APPROVER(S):	COUNTY BOARD OF SUPERVISORS		
VERSION:	1.0	PAGE:	PAGE **1** OF **2**

I. Standard Overview

The County of Santa Barbara requires employees to retain multiple passwords to access systems critical to their roles. The main point of storing your login credentials in a password manager is that doing so lets you use different, strong passwords for every use case. However, it's also important that you can get at your passwords from every one of your authorized or County-issued devices. Password manager applications and digital vaults need to adhere to NIST SP 800-63B Digital Identity Guidelines including but not limited to 256-bit AES encryption, zero knowledge architecture, and two-factor authentication. County Departments should encourage deployment of the Keeper tool in order to meet and remain current with respective regulatory requirements around password strength.

II. Standard Origin

NIST SP 800-63B

III. Scope

This County selected standard Password Management and Digital Vault tool, Keeper, should be used by anyone inputting passwords as the County and/or in support of the County. This includes employees, contractors, consultants, temporaries, and other workers at the County, including all personnel affiliated with third parties that access the County network.

IV. Definitions

1. Strong Password: NIST SP 800-63B defines authenticator assurance levels 1-3 and the County seeks to meet AAL2 standards and focus on the following current guidance:
    i. An eight character minimum and 64 character maximum length
    ii. The ability to use all special characters but no special requirement to use them
    iii. Restrict sequential and repetitive characters (e.g. 12345 or aaaaaa)
    iv. Restrict context specific passwords (e.g. the name of the site, etc.)
    v. Restrict commonly used passwords (e.g. p@ssw0rd, etc.)
    vi. **Restrict passwords obtained from previous breaches**

V. Standard Application

This standard will be applied as an original solution, and will replace all other solutions at their end of life.

I. Related Standards:

No standard exists

II. Referenced Documents:

https://pages.nist.gov/800-63-3/sp800-63b.html

http://www.keeper.com