COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	PASSWORD POLICY	ITEM NUMBER:	ITAM-0520
OWNER:	DEPARTMENT OF GENERAL SERVICES	ADOPTION DATE:	MM/DD/2019
APPROVER(S):	COUNTY BOARD OF SUPERVISORS	REVIEW DATE:	MM/DD/2022
VERSION:	1.2	PAGE:	PAGE **1** OF **3**

I. Purpose

This policy establishes the County of Santa Barbara standards for the creation of strong passwords, the protection of those passwords, and the frequency of change.

II. Audience

The audience for this policy is all County employees, contractors and third-parties who access County networks or systems.

III. Scope

This policy applies to anyone who has or is responsible for an account (or any form of access that supports or requires a password) on any County network or system.

IV. Definitions

1. Authorized Individuals: County employees, contractors, or any other individuals with authorized access to the information system in which the County has the authority to impose rules of behavior with regard to system access.

2. Information Technology (IT): the technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data.

3. IT Standards Committee: the governing body under the County's IT Governance Program that evaluates and recommends IT methods, processes and technologies that become a countywide standard.

4. Password: a word or other string of characters, kept secret or confidential, that must be supplied by a user in order to gain full or partial access to a computer, computer system, or electronic device.

5. Security Breach: any incident that results in unauthorized access of data, applications, services, networks, and/or devices by bypassing their underlying security mechanisms.

6. Strong Password: a password consisting of a length of at least 8 characters with at least one lowercase letter, one uppercase letter, one number and a non-alphanumeric special character such as a punctuation mark.

V. Policy

County of Santa Barbara employees, contractors and third parties must access a variety of IT resources, including computers and other hardware devices, data storage systems, and other accounts. Passwords are critical to IT security in assuring only authorized individuals can access those resources and data.

All authorized individuals who have access to any of those resources are responsible for choosing strong passwords and protecting their log-in information from unauthorized people. Compliance with this policy ensures County resources and data receive adequate password protection.

A. General Requirements:

- Individuals may never share their passwords with anyone else in the County, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.

- Individuals may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.

- All passwords that are no longer needed must be deleted or disabled immediately. These situations include but are not limited to:
  - When an employee retires, quits, is reassigned, released, dismissed, etc.
  - When an employee is out of the office for more than 30 days.
  - Default passwords shall be changed immediately on all equipment.
  - Contractor accounts, when no longer needed to perform their duties.

B. Storage of Passwords:

Individuals must not store their passwords in an unencrypted format for reference; refrain from writing passwords down or recording them in a readable format. However, employees may store passwords in repositories approved as a standard through the County IT Standards Committee.

C. Password Construct Requirements:

Password requirements vary depending on compliance and regulatory requirements assigned to the classification of information accessed. Password constructs will include attributes such as: character length, complexity, reuse, expiration, etc.

The County of Santa Barbara shall mandate password construct requirements as follows:

- Criminal Justice Information (CJI): Access to CJI data will require a password construct that adheres to the U.S. Department of Justice, Federal Bureau of Information *Criminal Justice Information Services (CJIS) Security Policy*. Further information may be found at the following link here.

- Federal Tax Information (FTI): Access to FTI data will require a password construct that adheres to U.S. Internal Revenue Service (IRS) *Publication 1075*. Further information may be found at the following link here.

- Health Insurance Portability and Accountability Act (HIPAA): Access to HIPAA data will require a password construct that adheres to the U.S. National Institute

of Standards and Technology (NIST). Further information may be found at the following link here.

- Payment Card Information (PCI): Access to PCI data will require a password construct that adheres to the *Payment Card Industry Data Security Standard (PCI DSS).* Further information may be found at the following link here.

- General Information: Access to general information within the County shall require a minimum secure password construct that adheres to the recommendations set forth by the County IT Standards Committee. Further information may be found at the following link here.

1. Applicable Rules, Laws, and Regulations:

   i. NIST Special Publication 800-63B, "Digital Identity Guidelines"

   ii. FBI Criminal Justice Information Services Security Policy

   iii. Health Insurance Portability and Accountability Act of 1996

   iv. IRS Publication 1075

   v. Payment Card Industry Data Security Standard

2. Exceptions: N/A

3. Non-Compliance: Employees who fail to adhere to this policy may be subject to administrative action that may include negative impacts to employee performance reviews. Additional civil and/or criminal penalties related to the breach of classified data may be applied from their respective legal regulatory bodies.

4. Related Policies: N/A

5. Referenced Documents: N/A

6. Revision History:

VERSION	CHANGE	AUTHOR	DATE OF CHANGE
1.0	Initial Release	Thomas Gresham	06/18/2018
1.1	Policy Committee Draft Revision	Thomas Gresham	08/13/2018
1.2	EITC requested modifications	Thomas Gresham	10/08/2018