Main Category

County Policy Format

County of Santa Clara

Administrative Policies & Procedures Manual

Category: Information Security Sub-category: Access

Policy Name: Local User Logon and Authentication

Policy Number: SCC-LULA

Business Owner Title: Chief Information Security Officer

1.0 Policy Purpose and Summary:

Purpose:

This policy describes user logon information, maintenance, and user authentication for users who attempt to access County owned computer resources. The policy applies to all individuals and/or organizations that use County information resources, including County employees, contractors, consultants, other government entities (*such as Federal, State, or other Counties*), and third-party vendors who access County systems for maintenance purposes.

Additional policies that deal with accessing County systems or data *remotely* (*from outside the County's network infrastructure*) are provided in Section 8.0 (*Remote Access*). Authentication and Authorization measures that apply specifically to application access are presented in Section 19.0 (*Application Security*).

County Policy Format

Policy:

4.1.1	Departments shall ensure only Users with legitimate needs to access County IT resources are provided with user accounts. A User's direct manager is responsible for initiating account(s) creation and account(s) termination if any unique processing is required. Otherwise, when a User leaves the County, TSS will automatically disable the account.	If you don't need it, you don't get it and direct managers need to play a role in account management
4.1.2	A user account shall be explicitly assigned to a single, named individual. No group or shared computer accounts or passwords are permissible except when necessary and warranted due to legitimate business needs.	It is your account with your name on the account
4.1.3	The level of authorization assigned to individual user accounts shall be restricted to only those privileges that are required by the User to perform legitimate County business processes.	Only the access necessary to do your job
4.1.4	At the time of network logon, the User shall be presented with a County-approved statement ("*login banner*") containing language regarding appropriate use of County computer systems.	Read the banner for logon requirements
4.1.5	All access to internal County computer systems shall be controlled by an Authentication method involving a minimum of a User Identifier (ID) and password combination that provides verification of the User's identity.	We need to know that your are the person logging in with your credentials
4.1.6	County approved password standards shall be applied for access to all County systems. This includes standards for "strong" passwords, frequency of password changes, password re-use, password distribution, and password protection.	Upper and lower case letters, numbers, special characters

4.1.7	Software as a Service (SaaS) solutions must utilize the latest Single Sign-On (SSO) capabilities and version. They must also integrate with the County's identity provider. If a SaaS solution is unable to comply with this requirement the Information Security Office can review to see if an exception is permitted.	Use the latest technology to benefit the end user and increase our cyber security posture

2.0 Related Policies:

General Security Policies	-	SCC-GSP
Remote Access	-	SCC-RAP
Data Classification	-	SCC-DC
Application Security	-	SCC-AS

3.0 Standards, Regulations, Statute Mapping

ISO27001:2005 standard as mapped to HIPAA, FedRamp, PCI, and NIST 800-53

4.0 Frequently Asked Questions/Scenarios:

Link to overall information security FAQs

5.0 Control Families and Controls:

- SCC-IA ○ IA - Identification and Authentication
    - IA-2 Organizational Users
    - IA-3 Device Identification and Authentication
    - IA-4 Identifier Management
    - IA-5 Authenticator Management
    - IA-6 Authenticator Feedback
    - IA-7 Crytpographic Module Authentication
    - IA-8 Non-Organizational Users
- SCC-AC Access Control
- SCC-APMEP – Elevate Privileges
- Managing Elevated Privileges on County Devices.docx

County Policy Format

Forms associated with policy: User Responsibility Statement

Countywide policy (*Yes*)

For internal use:

Version Number	Date	Changes made
1	5/8/2013	Removed roles and responsibilities -
2	1/15/2015	Reviewed for publication
3	Every November	Reviewed annually for updates and changes