



BOARD OF SUPERVISORS  
AGENDA LETTER

Agenda Number:

Clerk of the Board of Supervisors  
105 E. Anapamu Street, Suite 407  
Santa Barbara, CA 93101  
(805) 568-2240

**Department Name:** General Services  
**Department No.:** 063  
**For Agenda Of:** February 28, 2023  
**Placement:** Administrative  
**Estimated Time:**  
**Continued Item:** No  
**If Yes, date from:**  
**Vote Required:** Majority

---

**TO:** Board of Supervisors  
**FROM:** General Services Janette D. Pell, Director, 805-560-1011  
Contact Info: Chris Chirgwin, Chief Information Officer (CIO), 805-568-2608  
Andre Monostori, Deputy CIO, 805-568-2606  
**SUBJECT:** Countywide Information Technology (IT) Governance – All Districts

---

**County Counsel Concurrence**

As to form: Yes

**Auditor-Controller Concurrence**

As to form: No

**Other Concurrence:**

As to form:

**Recommended Actions:**

That the Board of Supervisors:

- a) Approve the following Standards; and
  1. Identity & Access Management (IAM)
  2. Login Identification (ID) & Display Name
  3. Device Naming
- b) Approve the following Information Technology (IT) Policy; and
  1. Remote Access (ITAM-0575)
- c) Determine that the above action is not a project under the California Environmental Quality Act (CEQA) pursuant to CEQA Guidelines Sections 15378(b)(4) and 15378(b)(5) because it consists of government administrative or fiscal activities that will not result in direct or indirect physical changes in the environment.

**Summary Text:**

In May 2018, the Countywide Information Technology (IT) Governance Program was established to provide high-level oversight and guidance regarding County IT investment activity. The Program exists to ensure cooperation, collaboration, and consensus-driven advice on information technology investment priorities for the County good. Governance is a framework consisting of a set of responsibilities and practices exercised by the County to provide strategic direction, ensure objectives are achieved, manage risk appropriately, and verify County resources are used responsibly.

## **Background:**

Historically, County governance has been driven by the need for the transparency of government risks and the protection of citizens. The pervasive use of technology has created a critical dependency on IT that calls for a specific focus on IT governance. The need to integrate information technology governance with overall management is similar to the need for information technology to be an integral part of the enterprise rather than discreet individual department efforts that run the risk of duplication, incompatibility, and financial inefficiencies.

To address this need, the Countywide Information Technology Governance Program was formed in May 2018. The Program aligns with the Renew 22 Initiative and the Countywide Information Technology Strategic Plan. The structure includes the formation of an executive group, underpinned by committees dedicated to specific functions in support of cooperative and consensus-driven management of IT strategic plan initiatives. These groups include the Executive IT Council, IT Policy Committee, IT Standards Committee, and Communities of Interest (CoIs).

The Executive Information Technology Council (EITC) is the standing body that provides high-level oversight and guidance regarding County IT investment activity. The Council makes informed decisions regarding the strategic direction for County IT deployment and recommends the priority sequence and funding levels for new IT initiatives/projects to be undertaken by any IT organization. Similarly, the Council approves recommended IT policies and standards proposed by the governance committees.

The Information Technology Policy Committee drafts policies and procedures for approval by the Council. The Policy Committee will evaluate proposals from IT stakeholders, launch fact-finding activities as needed, and recommend to the Council changes to County IT Administrative Manual. IT policies reflect an organization's logical progression from working in an ad-hoc manner to one where people are following common and consistent processes and assist the County in understanding how to execute IT activities such as solution procurement, technology frameworks, security requirements, etc.

The Information Technology Standards Committee evaluates and recommends the composition of the County's IT Architecture, including what constitutes County IT standards. The focus of the Standards Committee is technology management. The Standards Committee will evaluate proposals from IT stakeholders, launch fact-finding activities as needed, and recommend to the Council changes to County IT Enterprise Architecture. The Standards Committee will balance the need for departmental flexibility (more IT components to support), with the need for the County to manage support costs by limiting the scope and complexity of what technologies the County adopts as standard.

Communities of Interest are ad-hoc committees that provide stakeholders the opportunity to form partnerships to address a common set of business automation issues or opportunities. The goal of these communities is to make highly effective use of automation among standard business functions, as a forum for special interests within the IT governance model, and utilize synergistic partnerships to share the financial burden as well as obtain the benefits of collaboration in the development of automation solutions.

All recommendations from the Policy Committee, Standards Committee, and Communities of Interest will be presented and approved by the EITC. Periodically these recommendations will be given to the Board of Supervisors for final approval.

The following Standards have been presented to and approved by the EITC. It is requested that the Board approve the following Standards:

- Identity & Access Management (IAM) Standard
  - Establishes the County's Microsoft IAM technology as the single source of truth for

identity, with Microsoft Azure Active Directory (AD) as the standard identity provider (IdP) for cloud applications. An on-premise Microsoft AD will continue to be available as long as necessary.

- The scope of the standard applies to:
  - Any identity used to access the County or County resources
  - Any application/system used in support of County operations.

This includes, but is not limited to, computers, employees (current and former), contractors, consultants, temporaries, volunteers, interns, and other workers at the County, including all personnel affiliated with third parties.

- Login Identification (ID) & Display Name Standard
  - Standardizes the process for creating and managing Login ID's and Display Names; reduces complications that can occur from conflicting user names across platforms by consistently defining unique Login ID's; defines standard procedures for Login ID exceptions in cases where the normal standard isn't allowed on given systems; defines standard procedures for addressing duplicate Login ID's; defines a standard Display Name naming convention.
  - The scope of the standard applies to:
    - All County departments
    - Newly created accounts and/or current accounts when compliance is needed.
- Device Naming Standard
  - Defines a naming convention for newly added computer objects in AD to better identify devices by department. This standard will define the procedures of how to name a device joined to the domain.
  - The scope of the standard applies to:
    - All Countywide computer objects added to AD as defined in the standard.

The following Policy has been presented to and approved by the EITC. It is requested that the Board approve the following Policy:

- Remote Access Policy (ITAM-0575)
  - The purpose of the policy is to address the cybersecurity risks associated with remotely connecting to the internal County network from outside of the County network using non-standard and non-supported remote access tools.
  - The scope of the policy applies to:
    - All users that remotely connect to the internal County network from outside of the County network.

**Fiscal and Facilities Impacts:**

Budgeted: N/A

**Staffing Impacts:** None

**Special Instructions:** None

**Attachments:**

1. Attachment A – Identity & Access Management Standard

2. Attachment B – Login ID & Display Name Standard
3. Attachment C – Device Naming Standard
4. Attachment D – Remote Access Policy (ITAM-0575)

**Authored by:**

Jason Womack, Administrative Office Professional II