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 4, 2020
Placement:	Departmental
Estimated Tme:	30 Minutes
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: Thomas Gresham, Assistant Director (805) 568-2606

SUBJECT: **Countywide Information Technology Governance Program - All Districts**

County Counsel Concurrence	Auditor-Controller Concurrence
As to form: Yes	As to form: No

Other Concurrence:
As to form:

Recommended Actions:

That the Board of Supervisors:

a) Receive and file the update on the Countywide IT Governance Program Charter, Executive Information Technology Council Charter, Information Technology Policy Committee Charter, Information Standard Committee Charter, and IT Administrative Manual;

b) Approve the following Information Technology Policies;
1. IT Administrative Manual
2. Cybersecurity Training Awareness Policy
3. Password Policy
4. Information Security Incident Management Policy
5. Third-Party Information Security Policy
6. Acceptable Use Policy

c) Approve the following Standards; and
1. Incident Management
2. Password Manager Digital Vault

d) Determine that the proposed actions are related to general policy and procedure making and organizational or administrative activities of governments that will not result in direct or indirect physical changes in the environment and is therefore exempt from the California

Environmental Quality Act (CEQA) pursuant to CEQA Guideline section 15378 (b)(2) and (5).

Summary Text:

In May 2018, the Countywide Information Technology 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 (Attachment 1). 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) Charter (Attachment 2) and as background the EITC Policy (Attachment 3) 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 recommend 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 (Attachment 4) and as background the Information Technology Policy Committee Policy (Attachment 5). 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 (Attachment 6) and as background the Information Technology Standards Committee Policy (Attachment 7). 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 six policies have been presented and approved by the EITC. It is requested the Board approve the following policies:

1. IT Administrative Manual (Attachment 8). This policy establishes the Information Technology Administrative Manual (ITAM) as the authoritative repository for the cataloging of County Information Technology (IT) policies across all departments.

2. Cybersecurity Training Awareness Policy (Attachment 9). This policy establishes the requirement that individuals who access County networks or systems must complete annual cybersecurity awareness training.

3. Password Policy (Attachment 10). This policy sets the County of Santa Barbara standards for the creation of strong passwords, the protection of those passwords, and the frequency of change.

4. Information Security Incident Management Policy (Attachment 11). This policy establishes the requirements for activities related to responding to information security incidents at the County of Santa Barbara. The policy defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies, procedures and reporting requirements.

5. Third-Party Information Security Policy (Attachment 12). This policy establishes the security requirements for the use of third-parties that handle sensitive County data, either by storing, processing, transmitting, or receiving information.

6. Acceptable Use Policy (Attachment 13). This policy has been updated and establishes the permissible access and use of County Information Technology resources, ensuring consistency with County policies and any applicable compliance, regulatory, and legal requirements.

The following two standards have been presented and approved by the EITC. It is requested the Board approve the following standards:

1. Incident Management (Attachment 14). This standard identifies the ServiceNow platform to provide centralized IT incident management to ensure standardized IT incident response

procedures, risk-based prioritization of IT incident resolution, and countywide IT incident trending.
2. <u>Password Manager Digital Vault</u> (Attachment 15). This standard identifies the Keeper Security application to provide centralized password storage for the auditing, management, and protection of County credentials used to access systems and information.

Next Steps:

In the short term, the following steps will continue:
1. The EITC Program will continue to develop and bring new Policies and Standards to BOS for approval.
2. All IT projects will be reviewed for solutions with Countywide impact in mind and informed funding decisions will be made accordingly.
3. Implement recommendations from the IT Inventory and Assessment.
4. Implement recommendations from the IT Security Audit.
5. Identify gaps, prioritize needs for Infrastructure for FY 2020-21 budget.

Longer term, the findings from KPMG Operation and Performance Review – General Services, will be incorporated into the Countywide Technology Strategic Plan.

Fiscal and Facilities Impacts:

None at this time.

Staffing Impacts: None

Special Instructions:

None

Attachments:

1. Information Technology Governance Program
2. Executive Information Technology Council Charter
3. Executive Information Technology Policy (Background)
4. IT Policy Committee Charter
5. IT Policy Committee Policy (Background)
6. IT Standards Committee Charter
7. IT Standards Committee Policy (Background)
8. IT Administrative Manual
9. Cybersecurity Training Awareness Policy
10. Password Policy
11. Information Security Incident Management Policy
12. Third-Party Information Security Policy
13. Acceptable Use Policy
14. Incident Management

    15. Password Manager Digital Vault

<u>Authored by:</u>
Thomas Gresham, Assistant Director, General Services Department