BOARD OF SUPERVISORS
AGENDA LETTER

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

Agenda Number:

Department Name:	CEO
Department No.:	012
For Agenda Of:	September 21, 2021
Placement:	Administrative
Estimated Time:	
Continued Item:	No
If Yes, date from:	
Vote Required:	Majority

TO:	Board of Supervisors	
FROM:	CEO	Mona Miyasato, County Executive Officer, 568-3400 Janette D. Pell, Director, General Services 560-1011
	Contact Info:	Janette D. Pell, Director, General Services 560-1011
SUBJECT:	**Countywide Technical Cyber Security Policies – All Districts**	

County Counsel Concurrence
As to form: Yes

Auditor-Controller Concurrence
As to form: Yes

Other Concurrence: Risk Management
As to form: Yes

Recommended Actions:

It is recommended that the Board of Supervisors:

a) Approve the following 20 Technical Security Policies;
   1. IT Security Program Description (ITAM-0600);
   2. IT Security Program Implementation Plan (ITAM-0601);
   3. Glossary of IT Security Terms (ITAM-0602);
   4. Access Control (AC) (ITAM-0610);
   5. Awareness and Training (AT) (ITAM-0611);
   6. Audit and Accountability (AU) (ITAM-0612);
   7. Security Assessment and Authorization (CA) (ITAM-0613);
   8. Configuration Management (CM) (ITAM-0614);
   9. Contingency Planning (CP) (ITAM-0615);
   10. Identification and Authentication (IA) (ITAM-0616);
   11. Incident Response (IR) (ITAM-0617);
   12. Maintenance (MA) (ITAM-0618);
   13. Media Protection (MP) (ITAM-0619);
   14. Physical and Environmental Protection (PE) (ITAM-0620);
   15. Planning (PL) (ITAM-0621);
   16. Personnel Security (PS) (ITAM-0623);
   17. Risk Assessment (RA) (ITAM-0625);

18. System and Services Acquisition (SA) (ITAM-0626);
19. System and Communications Protection (SC) (ITAM-0627); and
20. System and Information Integrity (SI) (ITAM-0628); and

b) Determine that the above action is not a project under the California Environmental Quality Act (CEQA) pursuant to CEQA Guidelines Sections 15378(b)(2) and 15378(b)(5) because it consists of government administrative activities, including general policy or procedure making, that will not result in direct or indirect physical changes in the environment.

Summary Text:

The County of Santa Barbara completed a cyber security assessment and has developed a strong cyber security program based on foundational policies and procedures. The Information Technology Policy Committee drafted the attached Information Technology Cyber Security Policies. The IT Security Program is comprised of a series of Technical IT Security Policies (contained within the ITAM-06XX Series) that set forth a minimum level of security requirements that when implemented, will provide the confidentiality, integrity and availability of County Information Systems and County-owned data. Collectively these Technical Security Policies:

- Set the stage for appropriate behavior and awareness of acceptable IT security practices.
- Help IT staff across the organization to operate information-handling systems in a secure manner.
- Assist administrators and developers in the implementation and configuration of secure information-handling systems.
- Provide managers a means for determining whether new requirements are adhered to, or necessitate a change in, current policy.
- Assist the County in meeting compliance responsibilities.

These policies were presented to and approved by the Executive Information Technology Council, which in turn recommends approval by the Board of Supervisors. The Cyber Security Policies standardize the security policies for all County-deployed and -managed technology across all departments.

Background:

In May 2018, the Countywide Information Technology Governance Program (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.

The recent 'Insight' Assessment of Cyber Security in Santa Barbara County provided recommendations that included updating and standardizing cyber security policies for all County deployed and managed technology across all departments.

The policies presented here by the County IT Policy Committee and approved by the EITC are based on a mid-range approach to the National Institute of Standards and Technology (NIST) of cyber security for Federal, State, and Local public agencies. The maturing Countywide cyber security program will utilize these technical security policies to deploy appropriate and meaningful procedures that will enhance the protection of County technology assets including the protection of County data and information and strengthen its Federal and State compliance requirements.

The IT Security Program and associated Polices are based on NIST 800-53, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations.* NIST 800-53 is a framework and regulatory document, encompassing the processes and controls needed for a government-affiliated entity to comply with Federal Information Processing Standard (FIPS) 200.

The NIST (600) series of policies include:

ITAM Group #	**NIST Family**	**Policy Statement**
0610	Access Control (AC)	Access to County systems, data, and other resources is limited to only those authorized persons and things and that the level of such access granted is in accordance with County IT security policies, standards, and procedures, along with applicable State and Federal requirements.
0611	Awareness and Training (AT)	The appropriate level of information security awareness training is to be provided to all users of County IT.
0612	Audit and Accountability (AU)	County IT resources and information systems are to be established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance.
0613	Security Assessment and Authorization (CA)	County IT and the County's various business units (information owners) will ensure security controls in information systems, and the environments in which those systems operate, as part of initial and ongoing security authorizations, annual assessments, continuous monitoring, and system development life cycle activities.
0614	Configuration Management (CM)	County IT resources are to be inventoried and configured in compliance with County IT security policies, standards, and procedures, along with applicable State and Federal requirements.
0615	Contingency Planning (CP)	Normal County IT resources and information systems are to be available during times of disruption of services.
0616	Identification and Authentication (IA)	Only properly identified and authenticated users and devices are to be granted access to County IT resources in compliance with County IT security policies, standards, and procedures, along with applicable State and Federal requirements
0617	Incident Response (IR)	County IT and department IT are to properly identify, contain, investigate, remedy, report, and respond to computer security incidents.
0618	Maintenance (MA)	County IT resources are to be maintained in compliance with County IT security policies, standards, and procedures, along with all State and Federal requirements.
0619	Media Protection (MP)	Proper precautions are to be in place 1) to protect confidential information stored on media and 2) to control access to and dispose of media resources in compliance with County IT security policies, standards, procedures, and

		regulatory agreements, along with applicable State and Federal requirements.
0620	Physical and Environmental Protection (PE)	County IT resources are to be protected by physical and environmental security measures that prevent physical tampering, damage, theft, or unauthorized physical access.
0621	Planning (PL)	County IT resources and information systems are to be established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance.
0623	Personnel Security (PS)	Personnel security safeguards are to be applied to access and use information technology resources and data.
0625	Risk Assessment (RA)	County IT will perform risk assessments in compliance with County IT security policies, standards, and procedures.
0626	System and Services Acquisition (SA)	County IT resources and information systems are to be acquired with security requirements to meet the County information systems mission and business objectives.
0627	System and Communications Protection (SC)	System and communications protection for County Information Technology (IT) resources and information systems will be established and followed.
0628	System and Information Integrity (SI)	County IT resources and information systems are to be established with system integrity monitoring to include areas of concern such as malware, application and source code flaws, industry supplied alerts and remediation of detected or disclosed integrity issues.

These standard and industry accepted cyber security policies will provided security personnel the foundational security requirements and guidelines to ensure security compliance leading to a more protective environment of the County's technology assets from adverse cyber events.

Fiscal and Facilities Impacts:

Budgeted: N/A

Staffing Impacts: None

Special Instructions:

None

Attachments:

1. IT Security Program Description (ITAM-0600)
2. IT Security Program Implementation Plan (ITAM-0601
3. Glossary of IT Security Terms (ITAM-0602)
4. Access Control (AC) (ITAM-0610)
5. Awareness and Training (AT) (ITAM-0611

6. Audit and Accountability (AU) (ITAM-0612)
7. Security Assessment and Authorization (CA) (ITAM-0613)
8. Configuration Management (CM) (ITAM-0614)
9. Contingency Planning (CP) (ITAM-0615)
10. Identification and Authentication (IA) (ITAM-0616)
11. Incident Response (IR) (ITAM-0617)
12. Maintenance (MA) (ITAM-0618)
13. Media Protection (MP) (ITAM-0619)
14. Physical and Environmental Protection (PE) (ITAM-0620)
15. Planning (PL) (ITAM-0621)
16. Personnel Security (PS) (ITAM-0623)
17. Risk Assessment (RA) (ITAM-0625)
18. System and Services Acquisition (SA) (ITAM-0626)
19. System and Communications Protection (SC) (ITAM-0627)
20. System and Information Integrity (SI) (ITAM-0628)

Authored by:

Ray Aromatorio, Risk Manager