Attachment 1

IT Security Program Description – ITAM-0600

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	IT SECURITY PROGRAM DESCRIPTION	ITEM NUMBER:	ITAM-0600
OWNER:	DEPARTMENT OF GENERAL SERVICES	ADOPTION DATE:	MM/DD/20YY
APPROVER(S):	COUNTY BOARD OF SUPERVISORS	REVIEW DATE:	MM/DD/20YY
VERSION:	1.0	PAGE:	PAGE **1** OF **10**

I. Purpose

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.

II. Audience

The primary audience for the Technical IT Security Policies is Information Technology Professionals (County executives, managers, employees, contractors, vendors, and third parties) whose responsibilities include deploying, managing, administering, and operating all County Technology Assets (hardware, software, data systems, Cloud environments, SAAS, technology contracts, the Internet of Things (IOT), etc.).

III. Scope

The Technical IT Security Policies apply to any Information System that electronically generates, receives, stores, processes, or transmits County-owned data, whether the system is hosted on the County network or by a third-party provider. The Technical IT Security Policies are directed to all County technology personnel supporting the deployment of any technology assets in the County, including ‘on premise’, remotely, in the Cloud, Hosted, or otherwise, and includes hardware, software, application and environmental (hardware) services, application and database development and support, the Internet of Things (IOT), and all other technical aspects of County business.

Additionally, these provisions apply to anyone doing business as the County and/or in support of the County that is provisioned access to any County technology assets. This includes employees, contractors, consultants, temporaries, and other workers at the County, including all personnel affiliated with third parties, collectively referred to hereafter as “agents”.

IV. Definitions

See ITAM-0602, Glossary of Definitions

V. Policy

The Technical IT Security Policies are based on standards, best practices and other guidance published by the National Institute of Standards and Technology (NIST). The NIST framework was chosen since it is the Federal standard that has also been adopted by the State of California. The intent of adopting the NIST framework as the basis for the IT Security Program and Associated Polices is to aid in the creation of future MOUs and agreements between the State of California and County governments as well meeting all applicable State and Federal mandates.

The Technical IT Security 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.

Only applicable controls designed to protect systems with a ‘moderate’ category level, as defined in Federal Information Processing Standards publication (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, are included in the Technical IT Security Policies as a baseline.

The table below provides the primary policy statement for each of the Technical Policies:

ITAM	NIST Family	Technical 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	County IT and the County’s various business units (information owners) will ensure security controls in information systems, and the environments in which those

ITAM	NIST Family	Technical Policy Statement
	(CA)	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	County IT will perform risk assessments in compliance with County IT security policies, standards, and procedures.

ITAM	NIST Family	Technical Policy Statement
	(RA)	
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.

Minimum Requirements

Departments may set their own organizational policies, based on their individual business needs or specific legal requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), which may exceed the security requirements expressed in this Manual, but must, at a minimum, conform to the requirements.

The Technical IT Security Policies are superior to and supersede any other published policies to the extent the other policies provide a lesser security requirement.

Implementation Flexibility

Implementation of these policies and requirements, can, and may, lead to differing solutions and processes. It is the responsibility of all County IT professionals to meet these minimum policy security requirements regardless of the tools and solutions applied to these requirements.

Roles and Responsibilities

The following policy sets the minimum level of responsibility for the following individuals and groups:

- Central IT
- Departments
- Employees and Contractors

Additionally, the following mandatory/key roles and responsibilities that must be:

- Chief Information Security Officer
- Department Information Security Officer
- System Owner
- Computer Security Emergency Response Team (CSERT)

Central IT

The duties of Central IT include:

- Supporting IT governance and oversight for all applicable County Departments via the Countywide Information Technology Governance process.
- Developing, maintaining, and revising IT policies, procedures, and standards through the Countywide Information Technology Governance process.
- Providing guidance, technical assistance, and recommendations to the BOS, CEO, and Departments concerning IT matters.
- Developing and maintaining a Countywide IT master plan.
- Determining the feasibility of conducting regular external and internal vulnerability assessments and penetration testing to verify security controls are working properly and to identify weaknesses.
- Staffing the Computer Security Emergency Response Team (CSERT).
- Providing standards to be used in the procurement of IT services by or on behalf of the County and Departments.
- Maintaining a preapproved list of standardized hardware and software that meets the County standards for the enterprise that includes being security compliant.
- Maintaining a list of IT vendors that have passed all County security standards and policies to work on the County network.

Departments

Departments must provide clear direction and visible support for security initiatives and are responsible for:

- Initiating measures to assure and demonstrate compliance with the security requirements outlined in this policy.
- Implementing and maintaining an IT Security Program consistent with the Countywide program.
- Designating individuals for implementing and maintaining the Department’s security program.
- Ensuring that security is part of the information planning and procurement process.
- Determining the feasibility of conducting regular external and internal vulnerability assessments and penetration testing to verify security controls are working properly and to identify weaknesses.

- Implementing a risk management process for the life cycle of each critical IT system.
- Assuring the confidentiality, integrity, availability, and accountability of all Department information while it is being processed, stored, or transmitted electronically, and the security of the resources associated with those processing functions.
- Developing, implementing, and testing of an IT Disaster Recovery Plan along with a Business Continuity Plan/COOP Plan for critical IT Systems.
- Ensuring separation of duties and assigning appropriate system permissions and responsibilities for Department system users;

Employees and Contractors

All county employees and contract personnel are responsible for:

- Being aware of and complying with Countywide and Department policies for the protection of IT assets.
- Using IT resources only for intended purposes as defined by policies, laws, and regulations.
- Being accountable for their actions relating to their use of all IT Systems.

Chief Information Security Officer

The CISO manages the County's IT Security and Risk Management Program. The CISO has the following IT Security responsibilities:

- Develop, maintain, and oversee the County's IT Security Program.
- Monitor and report IT Security Program compliance.
- Serve as the IT security liaison to Central IT, Departments, and external organizations.
- Ensure sufficient resources are available to implement the County's IT Security Program in coordination with departments.
- Ensure that the County performs independent evaluations of the IT Security Program and its practices.
- Provide overall management and leadership and direction to the County IT Security Program.
- Assist and advise County and Department officials regarding their responsibilities for security.
- Report on the status of the County IT Security Program to the CEO, EITC, Department Executive Management, and other County officials.
- Consult with and brief the CEO, EITC, Department Executive Management, and other County officials regarding all critical information system security issues.
- Ensure managers for all IT resources are identified and that security authorization for those resources are accomplished within the planned time-frame.

- Determine the acceptable level of residual risk for an information subsystem and if an information subsystem will adequately protect sensitive information.
- Ensure County IT security planning and execution is practiced throughout the life cycle of each IT system.
- Ensure the Computer Security Emergency Response Team (CSERT) is staffed, trained, and maintained in a state of readiness.
- Ensure that persons with IT security responsibilities have appropriate role-based training.
- Establish an overall strategy for the County's IT Security Awareness and Training Program.
- Ensure the program is sufficiently staffed and funded to achieve its approved objectives in a timely manner.
- Ensure that the County's IT security policies, procedures, and standards are developed, approved, and maintained.
- Coordinate with the office of the Chief Executive Officer (CEO) and other senior management during security incidents with a moderate to high impact to the County that may include but are not limited to data breaches, theft, and damage to County assets.

Department Information Security Officer (DISO)

The DISO manages the department's IT Security and Risk Management Program. The DISO has the following primary IT security responsibilities:

- Develop, maintain, and oversee the department IT Security Program.
- Monitor and report IT Security Program compliance with these policies and other standards as appropriate.
- Serve as the IT security liaison to Central IT, CISO, and external organizations.
- Department resources with the assigned role as DISO may need specialized assistance with identifying, containing, reporting, and remediating security incidents.

System Owner

The System Owner (SO) has development and operational responsibility for the Information System. Multiple System Owners can be designated as required. However, each Information System must have at least one (1) assigned SO. The SO has the following primary responsibilities for IT Security:

- Determine and implement an appropriate level of security commensurate with the system sensitivity level.
- Perform risk assessments annually or as part of continuous monitoring activities to re-evaluate sensitivity of the system, risks, and mitigation strategies.
- Take appropriate steps to reduce or eliminate vulnerabilities after receiving the

results of continuous monitoring activities.

- Decide who has access to the system and grant individuals the fewest privileges necessary for job performance, re-evaluate the access privileges at least annually, and revoke access in accordance with guidelines upon personnel transfer, termination, or change in duties.
- Department system owners and related personnel will work in concert with the CISO and CSERT to ensure appropriate reporting procedures are documented and followed in the event that a security incident rises to the level of a security breach such as the loss of sensitive information to any appropriate regulating agency such as the State of California.

Computer Security Emergency Response Team (CSERT)

The Computer Security Emergency Response Team (CSERT) within Central IT will provide assistance to remediate security incidents and provide any needed coordination with law enforcement and other external incident response partners. CSERT will maintain standard processes and procedures for the handling of security incidents. CSERT serves as a single point of contact for security issues, coordinates incident response activities and performs assigned actions, which encompasses Continuous Monitoring, Situational Awareness, Event Management, and Incident Handling. The CSERT has the following additional IT Security responsibilities:

- Analyze and document Information Security incidents and security events.
- Perform investigations of potentially malicious or suspicious activity.
- Receive and monitor security alerts and advisories from US-CERT and take appropriate action in response to alerts and advisories.
- Report security incident information to senior Agency officials.
- Run periodic table top exercises to develop a ‘ready state’ CSERT.

Connotations

Use of the word “should” throughout this Manual should be interpreted to mean “shall” or “must,” (e.g., establishing a requirement).

“Central IT” describes the workgroup, services, and functions currently performed and housed within the ~~the~~ General Services, Information Communications & Technology (ICT) division.

Due to the nature the County’s decentralized IT operating structure the ownership/responsibility of specific systems/hardware is unknown at a policy level. Therefore, the Technical IT Security Policies may reference both Central IT and Department IT as responsible parties. As a practical matter the ownership/responsibility of the system/hardware determines the responsible party for compliance to the Technical IT Security Policy. Generally, for enterprise-wide systems Central IT will be primarily responsible and for other systems primary responsibility will be with the department or lead department when multi-department systems are involved.

VI. Exceptions

If a Department is unable to meet a required control, the CISO may grant an exception under the following conditions:

a. The Department consults with the CISO and provides sufficient justification, commensurate with the nature of the risk, for not meeting the security control requirements.

b. The Department consults with the CISO and develops a roadmap to implement the required security controls or alternate controls to satisfy the security objective commensurate with the risk. The roadmap and/or alternate controls must be approved and acknowledged by the CISO.

c. The Department develops a detailed project plan that identifies dates and milestones for all activities leading up to the remediation of the noncompliant security control.

When all conditions are met, the CISO will issue an exception to the Department for a defined period in which CISO will accept the risk(s) associated with the non-compliance. Additionally, the Department will provide progress updates to CISO every (6) months until the issue has been fully remediated. The CISO will report to the EITC annually or more frequently the status of all exceptions granted.

VII. Non-Compliance

Employees who fail to adhere to the policies within the IT Security Program may be subject to disciplinary action in accordance with civil service rules. Contractors and third parties that fail to adhere to these policies may face contractual penalties

VIII. References and Sources

1. Applicable Rules, Laws, and Regulations:

2. Related Policies:

   a. ITAM-0601 IT Security Program Implementation Plan

   b. ITAM-0901 Legacy IT Standards Exemption

3. Referenced Documents:

4. Revision History:

SUBJECT:	IT SECURITY PROGRAM DESCRIPTION	ITEM NUMBER:	ITAM-0600
OWNER:	DEPARTMENT OF GENERAL SERVICES	ADOPTION DATE:	MM/DD/20YY
APPROVER(S):	COUNTY BOARD OF SUPERVISORS	REVIEW DATE:	MM/DD/20YY
VERSION:	1.0	PAGE:	PAGE **10** OF **10**

VERSION	CHANGE	AUTHOR	DATE OF CHANGE
1.0	Initial Release	CISO/Policy Committee	08/25/2021