COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	THIRD-PARTY INFORMATION SECURITY POLICY	ITEM NUMBER:	ITAM-0540
OWNER:	DEPARTMENT OF GENERAL SERVICES	ADOPTION DATE:	MM/DD/2019
APPROVER(S):	COUNTY BOARD OF SUPERVISORS	REVIEW DATE:	MM/DD/2022
VERSION:	1.2	PAGE:	PAGE **1** OF **6**

I. Purpose

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.

II. Audience

The audience for this policy is all County employees, contractors or other parties authorized to acquire third-party services to handle County data.

III. Scope

This policy applies to County employees, contractors or other parties authorized to enter into any agreement or contract with third-parties who will be providing services that include the handling of County data. This policy also applies to instances where a third-party, their employees and any party within their supply chain may have indirect access to information i.e. staff/cleaners accessing rooms that may contain sensitive data.

IV. Definitions

A. Chief Information Security Officer (CISO): the CISO is a senior-level individual responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected

B. Data: a subset of information in an electronic format that allows it to be retrieved or transmitted.

C. Executive Information Technology Council (EITC): the overarching governing body chartered to provide high-level oversight and guidance regarding County IT investment activity

D. Information Technology (IT): the technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data

E. Sensitive Information: information that is protected against unwarranted disclosure requiring protections as mandated for legal, regulatory, ethical, privacy or proprietary considerations

F. Third-party: a supplier of goods or professional services which is independent of the customer

V. Policy

The purpose of this policy is to ensure that all contracts and agreements between the County and third-party suppliers have acceptable levels of information security and information governance processes to ensure that sensitive data is protected and managed in line with statutory and industry best practice requirements.

Information and information systems are vital County assets. It is essential that the organization has the appropriate technical and security measures in place to protect this information. This requirement becomes increasingly important in the case of medical records, law enforcement, financial payment & tax records and other sensitive information and where there is a need to share this information with third-parties who are delivering services on behalf of the County.

This policy outlines the process that must be followed prior to any contracts and/or agreements being entered into with a third-party by the County. It will provide assurance to the Board of Supervisors, County staff and constituents that every agreement or contract entered into meets appropriate technical and security measures to protect personal and/or sensitive information.

A. Third-party Selection

As part of the third-party selection process, County departments must ensure that the items listed below should be evaluated from a security perspective during the sourcing and contracting phases.

- company's reputation and history;
- quality of services provided to other customers;
- number and competence of staff and managers;
- financial stability of the company and commercial record;
- retention rates of the company's employees;
- quality assurance and security management standards currently followed by the company (e.g. certified compliance with CJIS, HIPAA, PCI, FTI).

- In relation to outsourcing, specifically, the risk assessment shall take due account of the:
  - nature of logical and physical access to County information assets and facilities required by the third-party to fulfill the contract;
  - sensitivity, volume and value of any information assets involved;
  - commercial risks such as the possibility of the third-party's business failing completely, or failing to meet agreed service levels;
  - security and commercial controls known to be currently employed by the County and/or by the third-party.

B. Preliminary Sensitive Data Sharing

Preliminary sharing of sensitive information is on occasion needed to facilitate quotations and other pre-engagement activities. The sharing of data is permitted provided that both parties sign the County's Non-Disclosure Agreement. Once this document is signed by the third-party and then countersigned by the County, the sharing of sensitive data may proceed.

C. Contractual Security Provisions

- A formal contract between County and the third-party shall exist. The contract shall clearly define the types of information exchanged and the purpose for so doing.

- If the information being exchanged is sensitive, a binding confidentiality agreement shall be in place between County and the third-party, whether as part of the outsource contract itself or a separate non-disclosure agreement (which may be required before the main contract is negotiated).

- Information shall be classified and controlled in according with County standards and/or policies.

- Any information received by the County from the third-party which is bound by the contract or confidentiality agreement shall be protected by appropriate classification and labeling as defined by the third-party.

- Upon termination of the contract, the confidentiality arrangements shall remain in perpetuity unless requested otherwise and agreed to by the County and third-party.

- All contracts shall be reviewed by County Counsel for accurate content, language and presentation.

- The contract shall specify successful completion of County security awareness training is required prior to the issuance of County network credentials to third-party personnel.

- The appropriate controls must be embedded or referenced within the contract, as applicable, such as:

  - Information security policies, procedures, standards and guidelines, as defined in CJIS, HIPAA, PCI, FTI or any other regulatory framework;
  - Background checks on employees or third-parties working on the contract;
  - Access controls to restrict unauthorized disclosure, modification or destruction of information, including physical and logical access controls, procedures for granting, reviewing, updating and revoking access to systems, data and facilities etc.;
  - Information security incident management procedures including mandatory incident reporting;
  - Return or destruction of all information assets by the third-party after the completion of the outsourced activity or whenever the asset is no longer required to support the outsourced activity;
  - Specification, design, development, testing, implementation, configuration, management, maintenance, support and use of security controls within or associated with IT systems, plus source code escrow;
  - Anti-malware, anti-spam and similar controls;

    - IT change and configuration management, including vulnerability management, patching and verification of system security controls prior to their connection to production networks;
    - The right of County to monitor all access to and use of County facilities, networks, systems etc., and to audit the third-party's compliance with the contract, or to employ a mutually agreed independent third-party auditor for this purpose. These audits include but are not limited to the following:
        - Information Security
        - Financial
        - Legal/Regulatory/Compliance
        - Personnel Screening
    - Termination of service shall ensure that all County data is portable and will be collected and returned to the County in a non-proprietary format or provide written certification of data destruction within a twenty-four (24) hour window;
    - Business continuity arrangements including crisis and incident management, resilience, backups and IT Disaster Recovery.

- For cloud service providers, in addition to the aforementioned controls, the following controls must also be embedded or referenced, as applicable, within the contract, such as:

    - Sensitive information compliance must be verified. Depending on the classification of data, cloud service providers must demonstrate compliancy with CJIS, HIPAA, PCI, FTI, etc.;
    - Personally Identifiable Information (PII) should be secured and verified by an independent security assessment of the cloud environment such as: SOC 2, ISO 27001 or FedRAMP certification;
    - Security incident reporting requires that the cloud provider report any security incidents related to physical or logical data compromises immediately to appropriate County personnel and take all appropriate actions to mitigate the security risk;
    - Data breaches requires that cloud providers notify the County within twenty-four (24) hours upon the discovery of a service provider security breach. Upon such notification, the County shall have the right, but not the obligation, to terminate the agreement with the cloud service provider. The provider shall pay for all costs incurred to remedy the breach for the County, its constituents, and related expenses related to the incident.

- Although third-parties that are certified compliant with CJIS, HIPAA, PCI, FTI can be presumed to have effective security, it may still be necessary for the County to verify security controls through the request of an auditing third-party attestation letter. For example, the handling of PCI should include a review of the third-party's PCI Attestation letter.

- The County Auditor-Controller is authorized by the Board of Supervisors and County Government Code to assess compliance with all County policies at any time.

- The County Auditor-Controller may assist with audits of outsourcing contracts including security compliance audits, and advise management on the risks and controls relating to outsourcing.

- Before the County can share Public Health Information (PHI) with a third-party, the third-party must sign a HIPAA "Business Associate Agreement."

D. Contractor and Consultant Personnel

- Contractors and consultants working on behalf of the County shall be subjected to background checks either through the contractor/consultant employer, or by the County department per that department's policies and procedures. Such screening shall take into consideration the level of trust and responsibility associated with the position and access to sensitive data such as criminal justice information or health records. Background checks may include, but are not limited to the following:
  - Proof of the person's identity (e.g. driver's license);
  - Proof of their academic qualifications (e.g. certificates);
  - Proof of their work experience (e.g. resume/CV and references);
  - Criminal record check;
  - Credit check.

- Companies providing contractors/consultants directly to the County or to other third-parties used by County, shall perform at least the same standard of background checks as those indicated above.

- The County will provide information security awareness training and education to all employees and third-parties working on the contract, clarifying their responsibilities relating to County information security policies, standards, procedures and guidelines (e.g. privacy policy, acceptable use policy, procedure for reporting information security incidents etc.) and all relevant obligations defined in the contract. Successful completion of security awareness training is required prior to the issuance of County network credentials.

E. Third-Party Procurement Checkpoints

- The CISO will review all IT contracts involving third-party access to County data for security risks prior to contract approval.

- The Procurement Chief will review all IT contracts involving third-party access to County data for inclusion of aforementioned contractual provisions.

1. Applicable Rules, Laws, and Regulations: N/A

2. Exceptions: N/A

3. Non-Compliance: County employees may face disciplinary action including the revocation of procurement authorization. Contractors and third-parties may face contractual

penalties for breach of contract.

4. Related Policies:

   i. ITAM-0510, Cybersecurity Awareness Training Policy
   ii. ITAM-0550, Acceptable Use Policy

5. Referenced Documents:

   i. County of Santa Barbara, Non-Disclosure Agreement
   ii. County of Santa Barbara, Business Associate Agreement (BAA)
   iii. County of Santa Barbara, Boiler Plate Agreement

Revision History:

VERSION	CHANGE	AUTHOR	DATE OF CHANGE
1.0	Initial Release	Thomas Gresham	03/15/2019
1.1	Incorporated Policy Committee Changes	Thomas Gresham	04/29/2019
1.2	Incorporated feedback from County Counsel in concurrence with the Policy Committee	Thomas Gresham	09/20/2019