Attachment A

ITAM-0550 Acceptable Use Policy

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	ACCEPTABLE USE POLICY	ITEM NUMBER:	ITAM-0550
OWNER:	INFORMATION TECHNOLOGY DEPT	ADOPTION DATE:	MM/DD/202Y
APPROVER(S):	COUNTY BOARD OF SUPERVISORS	REVIEW DATE:	MM/DD/20YY
VERSION:	3.0	PAGE:	PAGE **1** OF **6**

I. Purpose

The purpose of this policy is to establish guidelines for the acceptable use of information technology (IT) resources to ensure their integrity, security, and availability for all Authorized Users within the County. This policy aims to protect the County, its employees, contractors, volunteers, constituents, and taxpayers by defining the appropriate use of IT Resources.

II. Audience

This policy applies to all employees, contractors, volunteers, and any other individuals who are granted access to the County's IT Resources.

III. Scope

This policy covers all IT resources owned, leased, or operated by the County, including but not limited to computers, mobile devices, networks, software, data storage, and communication systems. It applies to on-site, remote, and mobile usage of these resources. It applies to any 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.

IV. Definitions

Authorized User: An individual or automated application or process that is authorized access to the resource by the system owner, in accordance with the system owner's procedures and rules.

User: Users include all employees, temporaries (including extra help and interns); volunteers of the County; contractors and vendors (including their employees and agents affiliated with the County); and any other authorized person utilizing County computing resources.

IT Resources: Includes hardware, software, networks, databases, internet access, and any other technology services or infrastructure provided by the County.

Sensitive Data: Information that is protected against unwarranted disclosure, including but not limited to personal data, financial data, and confidential business information.

See ITAM-0602, Glossary of Definitions for additional definitions.

V. Policy

It is the policy of the County Board of Supervisors that:

All Users are responsible for exercising good judgment regarding appropriate use of

information, computing resources, electronic devices, and network resources in accordance with the County's policies and standards, and all applicable laws and regulations (collectively "Applicable Laws"). All computing resources provided by the County or supported by the County are for the purpose of conducting the business of the County. It is the responsibility of each User of County computing resources to read, understand, and follow this policy. Questions concerning whether a particular use is acceptable or unacceptable shall be referred to the relevant department head or their designee.

1. General Use:
    - IT Resources are to be used for County business purposes. Incidental personal use is permitted, provided it does not interfere with job responsibilities or violate any other part of this or any other County policy.
    - Users must respect all Applicable Laws when using IT Resources.
    - Users must comply with all IT policies and procedures established by the County, as well as any department-specific policies related to their issued devices or access to IT resources. This includes, for example, a department's policy on the allowable use of personal mobile devices for email access. In the event of a conflict between policies, users are responsible for adhering to the most restrictive policy.

2. Security:
    - Users are responsible for safeguarding their authentication credentials (e.g., passwords, access tokens).
    - IT Resources must be used in a manner that protects against unauthorized access, viruses, malware, and other security risks.
    - Sensitive Data must be encrypted and securely stored according to the County's data protection policies.

3. Prohibited Activities:
    - Users must not engage in activities that are illegal, disruptive, or unethical, including, but not limited to, downloading pirated software, unauthorized scripting, accessing unauthorized systems, or distributing malware.
    - The use of IT Resources for personal gain, commercial activities not sanctioned by the County, or political purposes is prohibited.
    - Use of tools to gain unauthorized access to applications or information systems over the Internet or on County internal systems, including, but not limited to, use of VPNs to circumvent geofencing, is prohibited.
    - Additions or modifications to the County network without authorization, including, but not limited to, adding wireless access points or network switches, are prohibited.
    - Use of another person's user identification and password is prohibited.

4. Monitoring and Privacy:

- The County reserves the right to monitor and log all usage of its IT Resources to ensure compliance with this policy.
- Users have no expectation of privacy regarding their use of IT Resources.

5. Software and Hardware:
   - Only software and hardware approved by the County may be installed and used on its IT Resources.
   - Users must not attempt to modify or circumvent security settings or restrictions on IT Resources.

6. Reporting:
   - Users are required to immediately report to their supervisor or IT Department:
     - lost, stolen or misplaced devices
     - any known or suspected violations of this policy

7. Legal and Regulatory Compliance:
   - Users must comply with relevant legal and regulatory requirements, including, but not limited to, the California Public Records Act (CPRA), the California Consumer Privacy Act (CCPA), and the California Information Practices Act (IPA).
   - All electronic communications and documents created or received on County IT Resources may be subject to disclosure under the CPRA.
   - Users must handle personal data in compliance with the CCPA and the IPA, ensuring proper data protection and privacy measures.
   - Users must comply with all Applicable Laws, including, but not limited to, State laws and policies and local IT security ordinance & policies established by the County. This includes adhering to guidelines on data encryption, access control, incident reporting, and security training

8. Data Protection and Privacy:
   - Users must protect confidential information in accordance with all Applicable Laws.
     - Users must not store, copy or move any form of PII, PHI, PCI or other sensitive data onto any mobile device without explicit authorization.
   - In the event of a data breach, Users must follow the County's data breach notification procedures, including timely reporting to the affected individuals and relevant authorities.
   - Users are strictly prohibited from discussing any cyber event or breach with anyone outside the County and agency personnel directly responsible for managing the incident.
   - External communication restrictions:
     - No sharing of cyber event or breach details with the public, news media, or any non-County personnel without explicit authorization from the

County Executive Office (CEO), the County Public Information Officer (PIO), or the User's Department Director.

- The County CEO and the County PIO are the only authorized spokespersons permitted to release information related to a cyber event or breach on behalf of the County. This does not preclude required reporting by Department's to state and federal agencies with oversight responsibilities

9. Environmental Considerations:
   - Disposal of electronic waste (e-waste) must comply with California's Electronic Waste Recycling Act. Users must follow County procedures for the proper recycling and disposal of electronic devices.

10. Training and Awareness:
    - Users are required to participate in regular training sessions on IT security, data protection, and California privacy laws. The County will provide ongoing training to ensure Users are aware of current laws and best practices.

VI. Exceptions

1. Authorized Activities:
   - Certain Authorized Users, such as investigators, auditors, or IT security personnel, may be required to engage in activities that would otherwise be in violation of this policy in the course of their job duties and assignments. Such activities may include, but are not limited to, acquiring evidence in a criminal case, conducting security audits, or performing penetration testing.
     Such activities must be explicitly authorized by the appropriate departmental supervisory authority and documented in advance.
2. Compliance:
   - Authorized Users granted exceptions to this policy must ensure that their activities are conducted in compliance with all Applicable Laws and professional standards.
   - Any misuse of these exceptions will result in disciplinary action, up to and including termination of employment or contractual agreements.

VII. Non-Compliance

1. Consequences of Non-compliance:
   - Any User found to have violated this policy may be subject to disciplinary action in accordance with Civil Service Rules, up to and including termination of employment, contract termination, or legal action.
   - Inappropriate release (especially intentional) of data and information and unauthorized access to computing resources may constitute violation of civil and

criminal law which could result in penalties, fines and criminal sentences.
- Disciplinary actions will be determined based on the severity and frequency of the violation(s), as well as any previous history of non-compliance.

2. Investigation and Enforcement:
   - Reports of non-compliance will be investigated promptly and thoroughly by the appropriate supervisory authority or designated investigative team.
   - Users are expected to cooperate fully with any investigations into potential violations of this policy.

3. Remediation:
   - Users found to be in non-compliance may be required to undergo additional training on IT policies and procedures.
   - Depending on the nature of the violation, Users may also be required to take corrective actions to mitigate any harm or risk resulting from the non-compliance.

VIII. References and Sources

1. Applicable Rules, Laws, and Regulations:

   a. Health Insurance Portability and Accountability Act (HIPAA): Users must handle protected health information data in compliance with HIPAA. This includes ensuring proper security and privacy measures are in place to protect health information.

   b. California Public Records Act (CPRA): All electronic communications and documents created or received on County IT Resources may be subject to disclosure under the CPRA. Users must be aware that any records, including emails, created or stored using County IT Resources may be requested and made available to the public unless specifically exempted by law.

   c. California Consumer Privacy Act (CCPA): Users must handle personal data in compliance with the CCPA. This includes understanding the rights of individuals regarding their personal information and ensuring proper data protection and privacy measures are in place.

   d. California Information Practices Act (IPA): Users must ensure that any collection, maintenance, dissemination, and use of personal information adhere to the IPA. This includes maintaining the confidentiality and security of personal information.

   e. State of California Government Code 8314

   "(a) It is unlawful for any elected state or local officer, including any state or local appointee, employee, or consultant, to use or permit others to use public

resources for a campaign activity, or personal or other purposes which are not authorized by law…."

f. Civil Service Rule 1801 Political Activities of Officers & Employees

2. Related Policies:
   a. ITAM 0510 Cybersecurity Awareness Training
   b. ITAM 0520 Password
   c. ITAM 0530 Information Security Incident Management (being revised to Security & Privacy Incident Reporting)
   d. ITAM 0575 Remote Access
   e. ITAM 0602 Glossary of Definitions
   f. L1.1 Fraud, Theft, and Loss Policy

3. Revision History:

VERSION	CHANGE	AUTHOR	DATE OF CHANGE
1.0	Initial Release	Thomas Gresham	07/12/2019
2.0	Incorporated suggestions from Policy Committee and ICT	Thomas Gresham	08/30/2019
3.0	Full Revision	IT Policy Committee	MM/DD/YY